REDES INALÁMBRICAS EN LOS PAÍSES EN DESARROLLO

Una guía práctica para planificar y construir infraestructuras de telecomunicaciones de bajo costo



REDES INALÁMBRICAS EN LOS PAÍSES EN DESARROLLO

Cuarta Edición

Redes Inalámbricas en los Países en Desarrollo

Para más información sobre este proyecto puede visitar http://wndw.net
Primera edición: enero de 2006
Segunda edición: diciembre de 2007
Tercera edición: septiembre de 2008
Cuarta edición: octubre de 2013

 Como hemos descubierto que el mundo de las redes inalámbricas está a nuestro alrededor, los autores de este libro han incluido proyectos de América del Norte, del Sur, Europa, Asia, India y África. De esta manera tenemos que concluir que la mayoría de los sitios del mundo son capaces de aprovechar la información sobre instalaciones accesibles de redes tanto de interiores como de exteriores. Esperamos que disfruten de la lectura de este libro y lo utilicen como un punto de partida para iniciar un proyecto inalámbrico en su comunidad.

ISBN-13: 978-1492390855



ACERCA DEL LIBRO

La tercera edición del libro en inglés comenzó como un BookSprint en septiembre de 2011 en la hermosa ciudad de Copenhagen y tuvo como anfitrión a Sebastian Bütrich, uno de sus autores. Un equipo central de ocho personas finalizó luego la versión durante los meses siguientes hasta su publicación en marzo de 2013.
A lo largo del proyecto el grupo central ha buscado activamente contribuciones y estímulo de la comunidad mundial de instalaciones inalámbricas. Usted, como lector, puede darnos su propia contribución o plantear preguntas técnicas a los autores a través de nuestra página en Facebook:
https://www.facebook.com/groups/wirelessu

Este libro está disponible en forma de eBook para su dispositivo móvil, o para ser descargado gratuitamente desde su página http://wndw.net/ (en alta o baja resolución). También puede ordenarlo como impreso en:
http://www.lulu.com/

Proporcionamos una copia gratis en papel a todos los estudiantes que asisten a los entrenamientos en instalaciones inalámbricas impartidos por cualquiera de las instituciones con las que trabajamos tales como el International Centre for Theoretical Physics (ICTP), el Network Startup Resource Center (NSRC), el Asian Institute of Technology (AIT), la Internet Society (ISOC) y AirJaldi, para mencionar sólo algunos. Los invitamos encarecidamente a inscribirse en alguno de estos cursos en su región. Para información sobre cursos futuros, o si usted quisiera organizar un curso en su región, puede contactar a la editora, Jane Butler en:
janesbutler@networktheworld.org

Si usted está planificando un proyecto inalámbrico y necesita una copia de este libro porque no puede descargarlo por tener un ancho de banda limitado, o no está en capacidad de ordenarlo en línea, envíe, por favor, un mensaje electrónico o a través de Facebook a Jane y le enviaremos una copia en papel.

Colaboradores Principales

Jane Butler es la editora principal de esta versión del libro y actualmente es la Presidenta de la fundación privada networktheworld.org que promueve y apoya el crecimiento de la conectividad a Internet alrededor del mundo principalmente a través del respaldo de proyectos inalámbricos y entrenamientos.
Ver http://wirelessu.org. Jane es también la cabeza de la cooperación industrial y extensión de la University College London. Jane tiene un Honours Degree en Ingeniería, es Ingeniera Colegiada y miembro de la Institution of Electronics and Technology. Puede contactarla en: janesbutler@networktheworld.org

La editora expresa su reconocimiento y agradecimiento al grupo nuclear de autores que aparecen a continuación:

Ermanno Pietrosemoli. Ermanno es actualmente un investigador del Telecommunications/ICT for Development Lab del International Centre for Theoretical Physics (ICTP) de Trieste, Italia, y Presidente de la Fundación Escuela Latinoamericana de Redes "EsLaRed", organización sin fines de lucro que promueve las TIC en Latinoamérica a través de proyectos de entrenamiento y desarrollo. EsLaRed ganó en 2008 el premio Jonathan B. Postel Service Award otorgado por la Internet Society. Ermanno se ha dedicado a la implementación de redes inalámbricas de datos con un enfoque en las tecnologías de bajo costo y ha participado en la planificación y construcción de redes inalámbricas de datos en Argentina, Colombia, Ecuador, Italia, Lesotho, Malawi, México, Marruecos, Nicaragua, Perú, Trinidad, Estados Unidos y Venezuela. Ha sido expositor en numerosas conferencias y es el autor de muchos artículos relacionados con la transmisión de datos inalámbricos. Asimismo es coautor y editor técnico del libro Redes Inalámbricas en los Países en Desarrollo de descarga gratuita en http://wndw.net; Ermanno tiene un MSc. Degree de la Stanford University y fue profesor de Telecomunicaciones de la Universidad de Los Andes, Venezuela, del 1970 al 2000. Puede contactarlo en: ermanno@ictp.it

Marco Zennaro. Marco recibió su M.Sc. Degree en Electronic Engineering de la Universidad de Trieste, Italia. Defendió su tesis doctoral sobre *"Wireless Sensor Networks for Development: Potentials and Open Issues"* en el KTH-Royal Institute of Technology, Stockholm, Suecia.

Su área de investigación es en ICT4D, el uso de TIC para el Desarrollo. En particular está interesado en Redes Inalámbricas y en Redes de Sensores Inalámbricos en los países en desarrollo. Ha dado conferencias sobre tecnologías inalámbricas en más de veinte países. Cuando no está de viaje es el editor de wsnblog.com y puede contactarse en: mzennaro@ictp.it

Carlo Fonda es miembro de la Radio Communications Unit del Abdus Salam International Center for Theoretical Physics (ICTP) de Trieste, Italia. Carlo puede ser contactado en: cfonda@ictp.it

Stephen Okay. Steve es un friki por antonomasia con más de 20 años de experiencia en programación y administración de sistemas/redes y una pasión particular por los programas y redes abiertas/libres. Ha instalado redes inalámbricas en Laos, Malawi, Italia y Estados Unidos. Es un cofundador de Inveneo y ha dado entrenamiento sobre VoIP y redes inalámbricas en diversas instituciones alrededor del mundo. Vive y "hackea" en San Francisco, California, y puede ser contactado en: steve@inveneo.org

Corinna "Elektra" Aichele. Elektra ha estado trabajando intensamente sobre protocolos de redes de malla para la comunidad Freifunk de Alemania. Antes de la invención del protocolo de enrutamiento
B.A.T.M.A.N para redes inalámbricas de malla en 2006, trabajaba en el mejoramiento del protocolo de enrutamiento OLSR. Ella es una de las personas detrás del dispositivo Mesh-Potato, un robusto enrutador WiFi para exteriores de código y hardware abiertos. Elektra es parte de la comunidad Villagetelco que se dedica a implementar redes de malla para VoIP y datos. Vive en una casa con energía solar en Berlín, Alemania.
Su filosofía sobre la idea de comunicación ubicua para todos es: "El hecho de que hables en tu cabeza no significa que pienses sino sólo que estás hablando contigo mismo". A Elektra puedes contactarla en:
elektra@villagetelco.org http://villagetelco.org http://open-mesh.net/

Sebastian Büttrich. Sebastian es Research Lab Manager de la IT University de Copenhagen, http://pit.itu.dk
Trabaja con sistemas incrustados/penetrantes, tecnología inalámbrica, programas libres y de código abierto y energía solar para construir redes como gerente, creador, arquitecto, asesor e instructor.
Su trabajo se enfoca (pero no exclusivamente) en los países y comunidades en desarrollo, especialmente Asia y África.

Uno de sus enfoques actuales es el de desarrollar redes institucionales para investigación y educación con énfasis en la integración global y la sostenibilidad. Sus afiliaciones actuales son http://www.nsrc.org - the Network Startup Resource Center; http://wire.less.dk, una ONG y compañía cofundada con Tomas Krag; http://wirelessU.org, un grupo de profesionales dedicados a trabajar para una Sociedad de la Información inclusiva, mundial y basada en la gente; http://wndw.net/ como coautor del libro Redes Inalámbricas en los Países en Desarrollo. Sebastian tiene un doctorado en Quantum Physics de la Technical University of Berlin, Alemania, con un enfoque en óptica, radioespectroscopía, sistemas fotovoltaicos y programación científica. Le gusta la música y es músico; siente fascinación por el texto, el lenguaje y la poesía en sus múltiples formas. Puede contactarlo en: sebastian@less.dk

Jim Forster. Jim es un apasionado de difundir la Internet. Comenzó en Cisco en 1988 cuando era una compañía pequeña y pasó 20 años en ella, más que todo en IOS Software Development y System Architecture donde se convirtió en Distinguished Engineer.
Aún en Cisco, comenzó a trabajar en proyectos y políticas para mejorar el acceso a Internet en los países en desarrollo. En estos momentos está involucrado en esfuerzos con y sin fines de lucro para a extensión de las comunicaciones en África e India. Es el fundador de networktheworld.org, una fundación dedicada a mejorar las comunicaciones y la Internet, especialmente en África e India. Forma parte de varios Consejos de Directores, incluyendo Range Networks / OpenBTS e Inveneo en los Estados Unidos; Esoko Networks en Ghana, y AirJaldi de la India. Jim puede contactarse en: jforster@networktheworld.org

Klaas Wierenga. Klaas trabaja en el grupo Research and Advanced Development de Cisco Systems donde se enfoca en los tópicos de Identidad, Seguridad y Movilidad, a menudo en colaboración con la Comunidad de Investigación y Educación.
Es coautor del libro *Building the Mobile Internet* de la Cisco Press.
Antes de unirse a Cisco trabajaba en SURFnet, la Red Alemana de Educación e Investigación, donde creó el servicio móvil global WiFi para la academia llamado eduroam. Es también el Jefe de la Mobility Task Force de la Trans European Research and Education Networking (TERENA). Klaas participa en varios grupos de trabajo de la Internet Engineering Task Force (IETF) en las áreas de identidad, seguridad y

movilidad y dirige el grupo de trabajo abfab que trabaja con identidad federada para aplicaciones no-web.
Puede contactarlo en: klaas@wierenga.net

Eric Vyncke. Desde 1997 Eric trabaja como Distinguished Engineer de Cisco en el campo de seguridad ayudando a los clientes en la implementación de redes seguras. Desde el 2005 Eric también ha trabajado activamente en el área de Ipv6. Es el copresidente del Consejo Belga de Ipv6 y tiene una página muy conocida sobre monitoreo de implantes Ipv6: http://www.vyncke.org/ipv6status/. Es también Associate Professor de la University of Liège de Bélgica. Participa en varios grupos de trabajo de la Internet Engineering Task Force (IETF) relacionados con la seguridad o con Ipv6. Puede contactarlo en: eric@vyncke.org

Bruce Baikie. Bruce es miembro del equipo Broadband for Good de Inveneo en calidad de Director Senior de las Iniciativas de Banda Ancha (Broad Band Initiatives). Respaldado por su amplia experiencia en la industria de la energía y telecomunicaciones y por sus 16 años como experto en la industria de telecomunicaciones en la Sun Microsystems para asesorar la implementación de proyectos de Telecomunicaciones para el Desarrollo (ICT4D) con energía solar. Entre sus áreas de experticia se encuentran: redes inalámbricas, centros ecológicos de datos, sistemas de alimentación de corriente continua para equipos de telecomunicaciones y energía solar. Bruce ha publicado numerosos reportes y artículos sobre operación ecológica de centros de datos, y energía solar en Telecomunicaciones para el Desarrollo. Su educación incluye el grado de Ingeniero de la Universidad Tecnológica de Michigan y estudios avanzados en Empresas Internacionales de la Universidad de Wisconsin. Es también un conferencista invitado del Centro de Física Teórica Abdus Salam de Trieste, Italia, sobre las Telecomunicaciones para el Desarrollo (ICT4D) con energía solar. Durante los dos años pasados Bruce ha estado tutorizando estudiantes de ingeniería del Instituto Tecnológico de Illinois, de la Universidad de Colorado-Boulder, de la Universidad Estatal de San Francisco y la Universidad Estatal de San José, sobre el diseño de proyectos de Telecomunicaciones para el Desarrollo en Haití, Africa Occidental y Micronesia. Bruce puede ser contactado en:bruce@green-wifi.org

Laura Hosman. Laura es Assistant Professor de Ciencias Políticas del Instituto Tecnológico de Illinois. Antes de este trabajo, la Profesora Hosman

tuvo un cargo de investigadora postdoctoral de las universidades de California, Berkeley y Southern California (USC), respectivamente.
Tiene un doctorado de la USC en Economía Política y Política Pública.
Su investigación actual se enfoca en el papel de las tecnologías de la información y la comunicación (TIC) en los países en desarrollo, particularmente en términos de su efecto potencial sobre los factores socio-culturales, de desarrollo humano y de crecimiento económico.
Su trabajo se concentra en dos áreas principales: Asociaciones Público-Privadas y las TIC para la educación, ambas enfocadas en los países en desarrollo. Su bitácora, donde proporciona detalles sobre sus experiencias de trabajo, se encuentra en: http://ict4dviewsfromthefield.wordpress.com

Michael Ginguld. Fundador y Director de Estrategia y Operaciones de la Rural Broad Band Pvt. Ltd. Cofundador y Director General (CEO) de la Investigación e Innovación Airjaldi. Michael nació y fue criado en el Kibbutz Kissufim de Israel. Tiene más de 20 años de experiencia trabajando en proyectos sobre TIC, desarrollo rural y comunitario en la India, Indonesia, Cambodia Nepal e Israel. Michael ha trabajado en sectores con y sin fines de lucro en organizaciones nacientes y de base, grupos de apoyo, grandes ONG internacionales y en empresas comerciales de países desarrollados.
Michael trabajó y vivió en Dharamsala entre 1998 y 2002 y regresó a la India al comienzo de 2007 para incorporarse a una iniciativa de conectividad rural que finalmente condujo a la creación de la Airjaldi: Investigación e Innovación, una organización sin fines de lucro dedicada a R&D y al trabajo de formación de capacidades en el campo de las redes inalámbricas en el 2007; y de Banda Ancha Rural (RBB), un trabajo con fines de lucro sobre diseño, instalación, y gestión de redes de banda ancha para áreas rurales en 2009. Michael tiene un grado de Economía Agraria de la Universidad Hebrea de Jerusalén, Israel y un Máster en Estudios para el Desarrollo del Instituto de Estudios Sociales de la Haya, Países Bajos, así como un Máster en Administración Pública de la Kennedy School of Government, de la Universidad de Harvard, Cambridge, USA. Michael reside actualmente en Dharamsala, Himachal Pradesh, India, y puede ser contactado en: Michael@airjaldi.net

Emmanuel Togo. Emmanuel es de Ghana y obtuvo su primer título en Ciencias de la Computación y Física de la Universidad de Ghana en 1999. Actualmente es el Jefe de la Unidad de Redes del Sistema de Computación

de la Universidad de Ghana (UGCS). Es también uno de los miembros fundadores de la Red Académica y de Investigación de Ghana (GARNET), un equipo técnico que trabaja en la construcción de la red académica y de investigación de Ghana. Actualmente el objetivo de Emmanuel es el de diseño e implementación de una red académica inalámbrica, accesible, a grande escala que cubra todo el campus en Ghana. Se puede contactar en: ematogo@ug.edu.gh

The Open Technology Institute (que proporciona un caso de estudio para este libro) fortalece a los individuos y comunidades por medio de su investigación sobre políticas, aprendizaje aplicado e innovación tecnológica.

Respaldo

El equipo editorial hace un reconocimiento público a nuestro ilustrador técnico, Paolo Atzori, quien a lo largo de varios meses trabajó sin cansancio para garantizar que este libro tuviera ilustraciones magníficas, precisas y de fácil lectura. También se ha encargado de que se hayan publicado con éxito varias versiones del libro en formatos de alta y baja resolución.

Paolo Atzori. Paolo estudió Arquitectura en Venecia y Roma y Artes Audiovisuales en Colonia. Después de trabajar como arquitecto en Viena, Paolo colaboró con la Academia de Artes Audiovisuales de Colonia (KHM). En la Nueva Academia de Arte de Milán (NABA), fue nombrado Director del Máster en Diseño Digital Ambiental y Asesor del Programa doctoral del Colegio Planetario Nodo-M. Ha creado muchos proyectos artísticos y teatrales donde introduce novedosas representaciones del espacio caracterizadas por la dinámica de la ubicuidad y la interacción.
Paolo también ha trabajado como curador de exposiciones dedicadas al arte digital, ha dirigido programas educativos y publicado artículos y ensayos sobre cultura digital. Ha vivido y trabajado en Venecia, Roma, Nueva York, Viena, Colonia, Bruselas y Tel Aviv. Desde el 2005 vive en Trieste con su compañera Nicole y sus hijos Alma y Zeno. En 2011 fundó con Nicole Leghissa la agencia Hyphae. Sus contactos: http://hyphae.org http://www.xtendedlab.com/ http://www.khm.de/~Paolo

Autores y editores de versiones anteriores del libro:

Rob Flickenger. Rob ha escrito y editado varios libros sobre redes inalámbricas y Linux, como Wireless Hacks (O'Reilly) y Cómo Acelerar tu Internet (http://bwmo.net/). Está orgulloso de ser un friki informático, un científico loco amateur y un propulsor de redes libres en todo el mundo.

Laura M. Drewett es cofundadora de Adapted Consulting Inc., una empresa social que se especializa en la adaptación de la tecnología y en soluciones comerciales para el mundo en desarrollo. Desde el tiempo en que vivió en Mali en 1990 y escribió su tesis sobre programas educativos para niñas, Laura se ha dedicado a encontrar soluciones sostenibles para el desarrollo. Laura tiene un título con honores en Asuntos Extranjeros y Francés de la Universidad de Virginia y un certificado de Máster en Gerencia de Proyectos de la Escuela de Administración de la Universidad George Washington.

Alberto Escudero-Pascual y **Louise Berthilson** son los fundadores de IT +46, una compañía sueca de asesoramiento con enfoque en tecnología de la información en regiones en desarrollo.Más información en: http://www.it46.se/

Ian Howard. Después de volar alrededor del mundo durante siete años como paracaidista del ejército canadiense, Ian Howard decidió cambiar el fusil por un computador. Luego de finalizar su carrera en ciencias del ambiente en la universidad de Waterloo escribió en una propuesta lo siguiente: "La tecnología inalámbrica tiene la oportunidad de acortar la brecha digital. Las naciones pobres que no tienen como nosotros la infraestructura para la interconectividad, serán capaces de construir una estructura inalámbrica". Como premio, Geekcorps lo mandó a Mali como gerente del programa Geekcorps de Mali donde dirigió un grupo para equipar estaciones de radio con interconexiones inalámbricas y diseñó sistemas de compartir contenidos.

Kyle Johnston, http://www.schoolnet.na/

Tomas Krag ocupa su tiempo trabajando en wire.less.dk, organización sin fines de lucro basada en Copenhagen que fundó con su amigo y colega Sebastian Büttrich a comienzos del 2002. wire.less.dk se especializa en

soluciones inalámbricas de redes comunitarias con un enfoque especial en redes inalámbricas de bajo costo para el mundo en desarrollo. Tomas es también miembro de Tactical Technology Collective http://www.tacticaltech.org, organización sin fines de lucro basada en Amsterdam dedicada a "fortalecer movimientos sociales tecnológicos y redes en países en desarrollo y transición, así como a promover una sociedad civil que haga uso consciente, efectivo y creativo de las nuevas tecnologías." Actualmente sus esfuerzos se concentran en el proyecto Wireless Roadshow (http://www.thewirelessroadshow.org), que apoya miembros de la sociedad civil del mundo desarrollado para la planificación, implementación y mantenimiento de soluciones de conectividad basadas en espectro exento de licencia, y en tecnología y conocimiento abiertos.

Gina Kupfermann es ingeniera graduada en gestión de energía y tiene también un título en ingeniería y administración. Además de su profesión como contralora financiera ha trabajado para varios proyectos comunitarios auto-organizados y para varias organizaciones sin fines de lucro. Desde 2005 es miembro del consejo ejecutivo de la asociación de desarrollo para las redes libres, la entidad legal de freifunk.net.

Adam Messer. Su formación original es la entomología, pero Adam Messer sufrió una metamorfosis hacia las telecomunicaciones después de una conversación casual que en 1995 que lo llevó a fundar uno de los primeros ISP de África. Como pionero de los servicios inalámbricos para datos en Tanzania, Messer trabajó por 11 años en África del sur y del este en comunicaciones de voz y datos para nuevas empresas y compañías de celulares multinacionales. Hoy en día reside en Amman, Jordania.

Juergen Neumann (http://www.ergomedia.de) empezó trabajando con tecnologías de la información en 1984 y desde entonces ha estado buscando las distintas maneras de implementar las TIC de una manera útil para organizaciones y para la sociedad en general. En tanto asesor para implementación y diseño de estrategias de TIC ha trabajado para grandes compañías alemanas y de otros países así como para proyectos sin fines de lucro. En 2002 fue uno de los cofundadores de www.freifunk.net para la difusión del conocimiento y uso de redes sociales sobre redes abiertas y libres. Freifunk es globalmente considerado como uno de los proyectos comunitarios más exitosos del área.

Frédéric Renet es un cofundador de Soluciones Técnicas de la compañía Adapted Consulting, Inc. Fréderic se ha involucrado con TIC por más de 10 años y ha trabajado con computadores desde su infancia. Comenzó su carrera en TIC a comienzos de los noventa con un tablero de boletines (Bulletin Board System) sobre un módem analógico y desde entonces ha seguido creando sistemas que mejoran las comunicaciones. Más recientemente, Fréderic pasó más de un año en el IESC/Geekcorps de Mali como asesor. En esta función él diseñó varias soluciones innovadoras para la transmisión de radio FM, laboratorios de computación para escuelas y sistemas de alumbrado para comunidades rurales.

Prefacio a la edición en español

Esta cuarta edición del libro de redes inalámbricas es una versión en español de la tercera edición en inglés. Esto es debido a que después de la traducción de la segunda edición en inglés, realizada en diciembre de 2007, se hizo patente la necesidad de una actualización con la incorporación de casos de estudios enfocados a Latinoamérica, actualización que vio la luz como tercera edición en español en 2008.

Cinco años después, muchos aspectos de la tecnología han cambiado, por lo que es oportuna una revisión más profunda de los contenidos. Estos cambios se incorporaron a la tercera edición en inglés de 2013 editada por Jane Butler y con el aporte de nuevos autores, además de algunos de los que conformaron el equipo original, responsables de las ediciones anteriores.

La presente traducción estuvo a cargo de Lourdes González de Pietrosemoli, profesora de lingüística de la Universidad de los Andes de Mérida, Venezuela y fue revisada por Ermanno Pietrosemoli.

Ermanno Pietrosemoli

Contenido

INTRODUCCIÓN

Este libro tiene como objetivo capacitar a las personas para la construcción de redes de bricolaje (DIY) utilizando tecnologías inalámbricas. Ha sido compilado por un grupo de expertos que se ha dedicado al diseño, instalación y operación de redes inalámbricas durante un tiempo considerable, y que participa en la expansión del alcance de Internet en todo el mundo.

Creemos que las personas pueden tener una participación significativa cuando construyen sus propias infraestructuras de comunicaciones y pueden influir en la vasta comunidad que los rodea cuando garantizan que las redes son asequibles y accesibles. Esperamos no sólo convencerlo/la de que esto es posible, sino mostrarle cómo lo hemos hecho y proporcionarle la información y las herramientas necesarias para que usted comience un proyecto de redes en su comunidad local.

Cuando se le da a las personas de la comunidad un acceso rápido y barato a la información, ellas se beneficiarán directamente de lo que ofrece Internet. El tiempo y el esfuerzo que se ahorran al tener acceso a la red global de información se traducirá en un valor a escala local. Asimismo, la red se revaloriza a medida que más gente se conecta a ella. Las comunidades conectadas a la red a gran velocidad tienen una presencia en el mercado global donde las transacciones se suceden a la velocidad de la luz. La gente alrededor del mundo se ha dado cuenta de que el acceso a Internet les ha dado una voz para discutir de sus problemas, de política y de todo lo que es importante en sus vidas de una manera con la que ni el teléfono ni la televisión pueden competir. Lo que hasta hace poco parecía ciencia ficción, ahora se vuelve realidad, y esa realidad está construida sobre redes inalámbricas.

Un país llamado Aipotu

Imaginemos por un momento un país imaginario de nombre 'Aipotu' en el mundo en desarrollo. Aipotu ha estado conectado a Internet exclusivamente por medio de enlaces VSAT desde hace mucho tiempo.
Un día por fin llega la conexión por cable óptico submarino a las playas de Aipotu.

El desafío para Aipotu es ahora desarrollar desde cero una infraestructura de comunicaciones completa para todo el país.
La elección hoy en día es una estrategia de tres pasos. Primero, y antes que todo, Aipotu debería instalar líneas de fibra óptica donde le fuera posible. Estas líneas ofrecen la capacidad de transportar literalmente una modalidad de ancho de banda prácticamente sin límite. El costo de la fibra óptica es bajo si se tiene en cuenta su capacidad. Al actualizar los transceptores ópticos la capacidad de una línea de fibra óptica se incrementa sin instalar cables nuevos. Si Aipotu puede pagar el gasto de conexión de fibra óptica en cada hogar, no hay razón para no hacerlo. Si esto fuera así, nuestro modelo de tres pasos quedaría obsoleto y nos detendríamos aquí. Sin embargo, hay probablemente zonas de Aipotu que no pueden darse el lujo de las líneas de fibra óptica.

El segundo paso para que la gente de Aipotu pueda conectar poblados remotos o pequeñas ciudades es establecer enlaces punto a punto entre los puntos elevados. Es posible establecer enlaces de alta velocidad (40 Mbps) de 30 km o más entre torres de 20 metros de alto en terreno plano.

Si se dispone de cimas de montañas, edificios altos o colinas, se pueden hacer enlaces más largos. Los expertos en la tecnología de redes de Aipotu no tienen que preocuparse mucho por la tecnología inalámbrica que están instalando en las torres: el costo va a estar más bien en la construcción misma de las torres, la protección adecuada contra rayos, las fuentes de alimentación, energía de respaldo y protección antirrobo más bien que en el equipo inalámbrico en sí o en las antenas.

La tecnología de los tranceptores de radio avanza constantemente tal como la de los transceptores ópticos, pero un enlace inalámbrico a ser siempre de menor velocidad y capacidad que uno de fibra óptica.

El tercer reto para Aipotu es resolver el problema de la última milla: distribuir el acceso a todas las casas individuales, oficinas, instalaciones de producción etc. No hace mucho tiempo el método empleado era el de instalar cables de cobre pero ahora hay mejores soluciones. Este tercer paso de nuestro modelo de red es claramente del campo de la tecnología inalámbrica.

Propósito de este libro

El objetivo general de este libro es ayudarlo/la a construir tecnologías de la comunicación accesibles para su comunidad haciendo el mejor uso de cualquier recurso disponible.

Utilizando equipo económico ampliamente disponible es posible construir redes de alta velocidad de transmisión que conecten áreas remotas, proveer acceso de banda ancha donde ni siquiera existe la conexión por discado y conectarlo/la a usted y a sus vecinos a Internet. Utilizando materiales locales y fabricando partes usted mismo/a se pueden establecer enlaces de red confiables con muy poco presupuesto. Y al trabajar con su comunidad local se puede construir una infraestructura de telecomunicaciones que beneficie a todos los que participen en el proceso.

Este libro no es una guía para la configuración inalámbrica de su portátil o para seleccionar los productos adecuados a la red de su hogar, sino que trata sobre el armado de infraestructuras de red para que sean utilizadas como dorsales de redes inalámbricas de amplio alcance así como sobre la solución del problema 'de la última milla'. Teniendo presente estos objetivos, la información se presenta desde varios puntos de vista, incluyendo factores técnicos, sociales y económicos. Los estudios de casos analizados muestran los intentos hechos por varios grupos para la instalación de esas redes, los recursos utilizados y los resultados obtenidos en dichos intentos. Es importante notar que todos los recursos, técnicas y diseño de metodologías descritas en el libro son válidos en cualquier parte. Hay muchas zonas rurales en el mundo que todavía están desconectadas de Internet por razones económicas, geográficas, políticas, y otras.

La instalación de redes inalámbricas puede a menudo ayudar a solucionar estos problemas dando conexión a aquellos que aún no la tenían. Hay muchos proyectos de redes comunitarias surgiendo en todas partes. Sea que usted viva en el Reino Unido, en Kenya, en Chile, en India o en cualquier otro sitio del mundo, este libro puede ser una guía práctica útil.

Desde los primeros experimentos de transmisión de chispas a fines del siglo XIX, la inalámbrica ha sido un área de las tecnologías de la comunicación que ha evolucionado rápidamente.

Si bien en este libro proporcionamos ejemplos específicos de cómo construir enlaces de datos de alta velocidad, las técnicas descritas en el mismo no intentan reemplazar las estructuras cableadas existentes (como el sistema telefónico y las dorsales de fibra óptica).

Más bien, estas técnicas permiten incrementar la capacidad de esos sistemas y proporcionar conectividad en áreas donde la fibra u otro tipo de cable son una solución poco práctica.
Esperamos que este libro le sea útil para solucionar sus necesidades específicas de comunicación.

Incorporar una red inalámbrica a una red preexistente

Si usted es administrador(a) de redes se preguntará cómo insertar una red inalámbrica en su estructura de red actual.
La tecnología inalámbrica puede ayudar en muchas formas: desde ser una simple extensión (como una ampliación del alcance de una red Ethernet cableada a varios kilómetros) hasta ser un punto de distribución (un gran concentrador).
Aquí les presentamos algunos ejemplos de cómo su red puede beneficiarse de la tecnología inalámbrica.

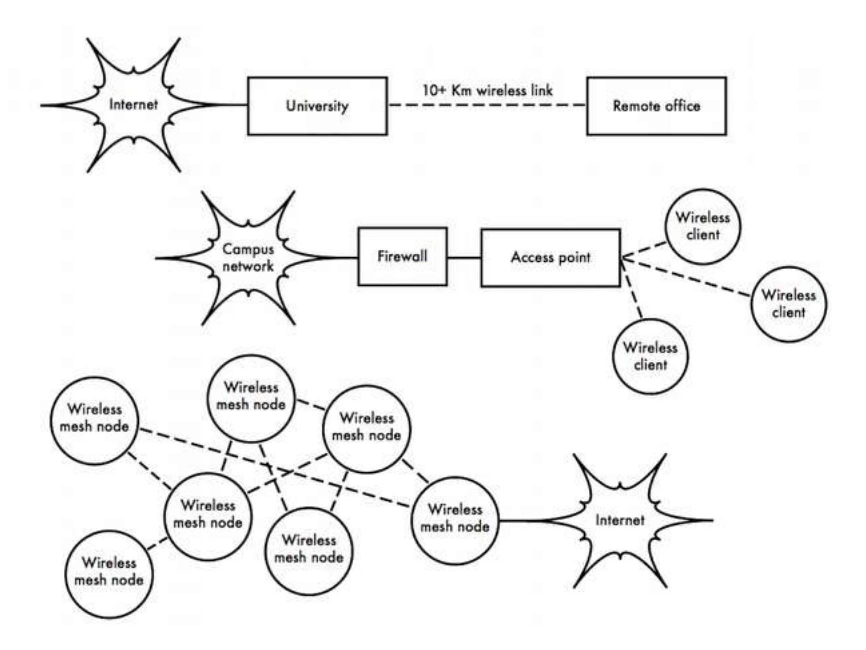


Figura I 1: Algunos ejemplos de redes inalámbricas.
Campus network: red del campus; firewall: cortafuegos; access point: punto de acceso; wireless client: cliente inalámbrico; wireless mesh node: nodo inalámbrico en malla

Organización del libro

Este libro tiene 4 secciones principales llamadas:

Física
Redes
Planificación e Instalación
Mantenimiento, Monitoreo y Sostenibilidad

Al final encontrará las secciones **Glosario**, **Apéndices** y **Estudio de Casos.**

En las 4 secciones principales hay capítulos escritos por expertos claves con conocimientos teóricos y experiencia práctica en los tópicos correspondientes.

Hay un amplio rango de tópicos en los capítulos que son claves para que usted comience y desarrolle una instalación inalámbrica real en su comunidad. Otra fuente útil la encuentra en:

http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html

Este es la colección de materiales de las presentaciones empleadas por el mismo conjunto de expertos en sus actividades de entrenamiento en redes inalámbricas alrededor del mundo.
Además, los expertos autores de este libro consultan a menudo nuestra página de Facebook. En el proceso de construir su enlace, usted puede hacer preguntas en nuestra página. Respondemos con rapidez.

https://www.facebook.com/groups/wirelessu

FÍSICA

1. FÍSICA DE RADIO

Las comunicaciones inalámbricas hacen uso de las ondas electromagnéticas para enviar señales a través de largas distancias. Desde la perspectiva del usuario, las conexiones inalámbricas no son particularmente diferentes de cualquier otra conexión de red: el navegador web, el correo electrónico y otras aplicaciones funcionan como uno lo espera. Pero las ondas de radio tienen algunas propiedades inesperadas en comparación con una red cableada Ethernet. Por ejemplo, es muy sencillo ver el trayecto de un cable Ethernet: localice el conector de su computadora, siga el cable hacia el otro extremo, ¡y lo habrá encontrado! También se puede confiar en que colocar muchos cables Ethernet uno al lado del otro no va a causar problemas, ya que los cables confinan efectivamente las señales dentro del cable mismo.

Pero ¿cómo saber por dónde están circulando las ondas emanadas de su dispositivo inalámbrico? ¿Qué sucede cuando esas ondas rebotan en los objetos de la habitación u otros edificios en un enlace en exteriores? ¿Cómo pueden utilizarse varias tarjetas inalámbricas en la misma área sin interferir unas con otras?

Para construir enlaces inalámbricos estables de alta velocidad es importante comprender cómo se comportan las ondas de radio en el mundo real.

¿Qué es una onda?

En general estamos familiarizados con las vibraciones u oscilaciones de varias formas: un péndulo, un árbol meciéndose con el viento, las cuerdas de una guitarra, son todos ejemplos de oscilaciones.

Lo que tienen en común es que algo, un medio o un objeto, está oscilando de forma periódica con cierto número de ciclos por unidad de tiempo. Este tipo de onda a veces es denominada onda mecánica, puesto que son definidas por el movimiento de un objeto o de su medio de propagación.

Cuando esas oscilaciones viajan (esto es, cuando no están confinadas a un lugar) hablamos de ondas propagándose en el espacio. Por ejemplo, un cantante crea oscilaciones periódicas de sus cuerdas vocales al cantar. Estas oscilaciones comprimen y descomprimen el aire periódicamente, y ese cambio periódico de la presión del aire sale de la boca del cantante y viaja a la velocidad del sonido. Una piedra arrojada a un lago causa una alteración que viaja a través del mismo como una onda. Una onda tiene cierta velocidad, frecuencia y longitud de onda.

Las mismas están conectadas por una simple relación:

Velocidad = Frecuencia * Longitud de Onda

La longitud de onda (algunas veces llamada **lambda**, **λ**) es la distancia medida desde un punto en una onda hasta la parte equivalente de la siguiente, por ejemplo desde un pico de la onda hasta el siguiente. La frecuencia es el número de ondas enteras que pasan por un punto fijo en un segundo. La velocidad se mide en metros/segundos, la frecuencia en ciclos por segundos (o hertzios, representado por el símbolo ***Hz***), y la longitud de onda en metros.
Por ejemplo, si una onda en el agua viaja a un metro por segundo y oscila cinco veces por segundo, entonces cada onda tendrá veinte centímetros de largo:

1 metro / segundo = 5 ciclos / segundos * **λ**
λ = 1 / 5 metros
λ = 0,2 metros = 20 cm

Las ondas también tienen una propiedad denominada ***amplitud***. Esta es la distancia desde el centro de la onda hasta el extremo de uno de sus picos, y puede ser asimilada a la "altura" de una onda de agua. La relación entre frecuencia, longitud de onda y amplitud se muestran en la figura FR 1.
time.

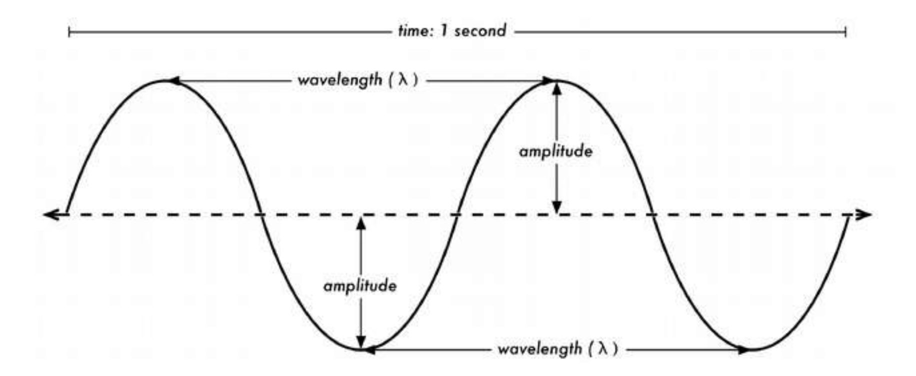


Figura FR 1: Longitud de onda (wavelength), amplitud, y frecuencia. Para esta onda la frecuencia es 2 ciclos por segundo, o 2 Hz; mientras que la velocidad es de 1 m/s

Las ondas en el agua son fáciles de visualizar. Simplemente tire una piedra en un lago y verá las ondas y su movimiento a través del agua por un tiempo. En el caso de las ondas electromagnéticas, la parte que puede ser más difícil de comprender es: ¿qué es lo que está oscilando?
Para entenderlo, necesitamos comprender las fuerzas electromagnéticas.

Fuerzas electromagnéticas

Las fuerzas electromagnéticas son fuerzas entre cargas y corrientes eléctricas. Nos percatamos de ellas cuando tocamos la manija de una puerta después de haber caminado en una alfombra sintética, o cuando rozamos una cerca eléctrica. Un ejemplo más poderoso de las fuerzas electromagnéticas son los relámpagos que vemos durante las tormentas eléctricas.
La ***fuerza eléctrica*** es la fuerza entre cargas eléctricas.
La ***fuerza magnética*** es la fuerza entre corrientes eléctricas.

Los electrones son partículas que tienen carga eléctrica negativa. También hay otras partículas cargadas, pero los electrones son los responsables de la mayor parte de las cosas que necesitamos conocer para saber cómo funciona un radio. Veamos qué sucede en un trozo de alambre vertical en el cual empujamos los electrones de un extremo a otro periódicamente. En cierto momento, el extremo superior del alambre está cargado negativamente — todos los electrones están acumulados allí.
Esto genera un campo eléctrico que va de positivo a negativo a lo largo del alambre.
Al momento siguiente, los electrones se han acumulado al otro lado y el campo eléctrico apunta en el otro sentido. Si esto sucede una y otra vez, los vectores de campo eléctrico, (que se representan por flechas que van de positivo a negativo) se desprenden del alambre y son radiados en el espacio que lo rodea. Lo que hemos descrito se conoce como dipolo (debido a los dos polos, positivo y negativo), o más comúnmente ***antena dipolo***. Esta es la forma más simple de la antena omnidireccional. El movimiento del campo electromagnético es denominado comúnmente ***onda electromagnética*** porque también hay un campo magnético asociado.
Un campo eléctrico en movimiento, como el de una onda, siempre está asociado con un campo magnético: no se presenta uno sin el otro. ¿Por qué es esto así?

Un campo eléctrico es causado por objetos cargados eléctricamente.
Un campo eléctrico en movimiento es producido por objetos móviles cargados eléctricamente, como hemos descrito en el ejemplo de la antena dipolo. Dondequiera que haya cargas eléctricas en movimiento, estas inducen un campo magnético.
Matemáticamente esto se formula en la ecuación de Maxwell: https://es.wikipedia.org/wiki/Ecuaciones_de_Maxwell
Puesto que los componentes eléctrico y magnético están conectados de esta manera, hablamos de un campo electromagnético.
En la práctica de instalación de redes inalámbricas, nos enfocamos en el componente eléctrico, pero también hay siempre un componente magnético.

Volvamos a la relación:
*Velocidad = Frecuencia * Longitud de Onda*

En el caso de las ondas electromagnéticas, la velocidad **c** es la velocidad de la luz.

$$c = 300.000\ km/s = 300.000.000\ m/s = 3*10^8\ m/s$$

$$c = f * \lambda$$

Las ondas electromagnéticas difieren de las mecánicas en que no necesitan de un medio para propagarse. Las mismas se propagan incluso en el vacío del espacio.
La luz de las estrellas es un buen ejemplo: nos llega a través del vacío del espacio.

Símbolos del sistema internacional de unidades

En física, matemáticas e ingeniería a menudo expresamos los números como potencias de diez. Repasaremos de nuevo estos términos y los símbolos usados para representarlos, por ejemplo gigahercio (GHz), centímetros (cm), microsegundos (µs), etc.
Estos símbolos forman parte del sistema internacional de medidas **SI** (*The International System of Units*) (http://www.bipm.org/utils/common/pdf/si_brochure_8_en.pdf). No son abreviaturas y no deben cambiarse.

El uso de mayúsculas o minúsculas es significativo, por lo tanto no debe ser alterado.

Símbolos SI

atto	10^{-18}	1/1000000000000000000	a
femto	10^{-15}	1/1000000000000000	f
pico	10^{-12}	1/1000000000000	p
nano	10^{-9}	1/1000000000	n
micro	10^{-6}	1/1000000	μ
mili	10^{-3}	1/1000	m
centi	10^{-2}	1/100	c
kilo	10^{3}	1000	k
mega	10^{6}	1000000	M
giga	10^{9}	1000000000	G
tera	10^{12}	1000000000000	T
peta	10^{15}	1000000000000000	P
exa	10^{18}	1000000000000000000	E

Conociendo la velocidad de la luz, podemos calcular la longitud de onda para una frecuencia dada.

Tomemos el ejemplo de la frecuencia para redes inalámbricas del protocolo 802.11b, la cual es:

f = 2.4 GHz = 2 400 000 000 ciclos / segundo

longitud de onda $(\lambda) = c / f$
$= 3*10^{8} / .,4*10^{9}$
$= 1.25*10^{-1}$ m
= 12.5 cm

La frecuencia, y, por tanto la longitud de onda determinan casi todo el comportamiento de una onda electromagnética. Gobierna las dimensiones de las antenas que construimos así como el efecto de las interacciones con los objetos que están en la trayectoria de propagación, incluyendo los efectos biológicos en los seres vivientes.

Los estándares inalámbricos se diferencian por supuesto por otros factores además de la frecuencia a la que funcionan. Por ejemplo, 802.11b, 802.11g y 802.11n pueden todos funcionar a 2.4 GHz, sin embargo, son muy diferentes entre sí.

En el capítulo sobre ***Telecomunicaciones Básicas*** discutiremos técnicas de modulación, técnicas de acceso a medios y otros puntos relevantes de los estándares de comunicaciones inalámbricas.
Sin embargo, las propiedades básicas que tienen las ondas electromagnéticas de penetrar los objetos, viajar largas distancias y otras, van a estar determinadas sólo por la física.
La onda electromagnética no sabe o es indiferente a la modulación, el estándar o la técnica empleada. Así que, mientras los diferentes estándares pueden implementar técnicas avanzadas para tratar la transmisión en ausencia de línea de vista *(Non Line of Sight: NLOS),* multitrayectoria u otros problemas, esas técnicas no pueden todavía hacer que una onda atraviese una pared si la pared está absorbiendo la frecuencia respectiva.
De esta manera, entender las bases del concepto de frecuencia y longitud de onda ayuda mucho en el trabajo práctico de redes inalámbricas.

Fase

Más adelante en este capítulo hablaremos de conceptos como interferencia, multitrayectoria, y zonas de Fresnel.
Para entenderlos necesitamos saber sobre la ***fase*** de una onda, o mejor dicho, sobre las ***diferencias de fase*** entre ondas.
Mire la onda senoidal de la figura siguiente; ahora imagine que tenemos dos ondas como esa moviéndose.
Ellas podrían estar exactamente en la misma posición: donde está el pico de una, está también el pico de la otra. En este caso decimos que están en fase, o que su diferencia de fase es cero. Pero una de las ondas podría estar desplazada respecto a la otra; por ejemplo, su pico podría estar donde la otra está en cero.

En este caso, tenemos una diferencia de fase.
Esta diferencia puede expresarse en fracciones de longitud de onda, por ej. $\lambda/4$, o en grados, por ej. 90 grados: un ciclo completo de la onda son 360 grados. Una diferencia de fase de 360 grados es lo mismo que una de 0 grados: no hay diferencia de fase.

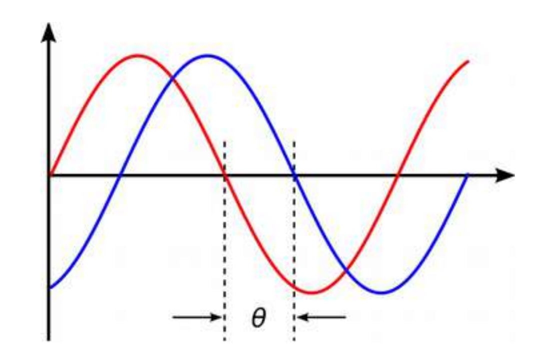


Figura FR 2: Diferencia de fase entre dos ondas

Polarización

Otra cualidad importante de las ondas electromagnéticas es la ***polarización***. La polarización describe la dirección del vector del campo eléctrico.

En una antena dipolo alineada verticalmente (el trozo de alambre recto), los electrones sólo se mueven de arriba a abajo, no hacia los lados (porque no hay lugar hacia donde moverse) y, por consiguiente, los campos eléctricos sólo apuntan hacia arriba o hacia abajo verticalmente.

El campo que se desprende del alambre y viaja como una onda tiene una polarización estrictamente lineal (y en este caso, vertical).

Si acostamos la antena en el suelo (horizontal) tendremos una polarización lineal horizontal.

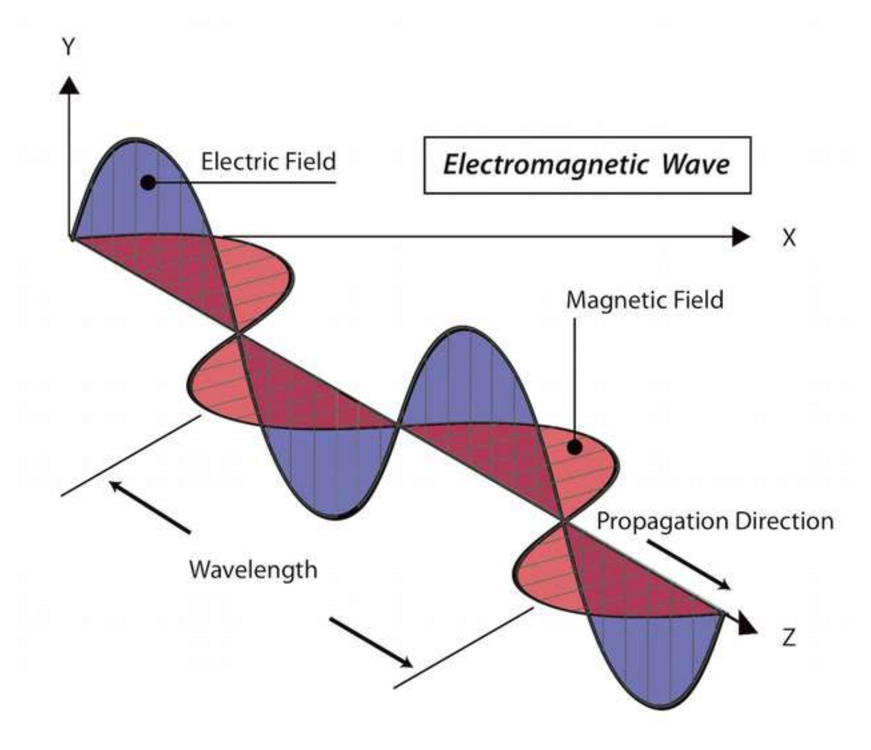


Figura FR 3: Onda electromagnética polarizada verticalmente

La polarización lineal es sólo un caso especial y nunca es tan perfecta: en general, siempre tendremos algunos componentes del campo apuntando hacia otras direcciones.

Si combinamos dos antenas dipolo iguales alimentadas con la misma señal, podemos generar una onda polarizada circularmente en la cual el vector del campo eléctrico se mantiene rotando perpendicularmente a la trayectoria de la onda. El caso más general es el de la polarización elíptica, en la cual el valor máximo del vector del campo eléctrico no es el mismo en las direcciones vertical y horizontal. Como podemos imaginar, la polarización se vuelve importante cuando se alinean las antenas.
Si se ignora, vamos a obtener una señal muy pequeña aún con la mejor de las antenas. A esto se llama desadaptación de polarización.
De la misma manera, la polarización puede ser usada de manera inteligente para mantener dos enlaces inalámbricos independientes y sin interferencia incluso cuando usen los mismos extremos (o compartan el mismo reflector)

y por ende la misma trayectoria: si uno de los enlaces está polarizado verticalmente y el otro horizontalmente, no van a "verse" entre sí. Esta es una manera conveniente de duplicar la tasa de datos en un enlace usando la misma frecuencia.

Las antenas que se usen en este tipo de aplicaciones deben construirse cuidadosamente con la finalidad de rechazar polarizaciones "no deseadas": es decir, una antena destinada a la polarización vertical no debe recibir o transmitir ninguna señal polarizada horizontalmente o viceversa. Lo expresamos como que deben tener rechazo de "polarización cruzada".

El espectro electromagnético

Las ondas electromagnéticas abarcan un amplio rango de frecuencias (y, correspondientemente, de longitudes de onda). Este rango de frecuencias y longitudes de onda es denominado ***espectro electromagnético***. La parte del espectro más familiar a los seres humanos es probablemente la luz, la porción visible del espectro electromagnético.

La luz se ubica aproximadamente entre las frecuencias de $7.5*10^{14}$ Hz y $3.8*10^{14}$ Hz, correspondientes a longitudes de onda desde cerca de 400 nm (violeta/azul) a 800 nm (rojo).

Normalmente también estamos expuestos a otras regiones del espectro electromagnético, incluyendo los campos de la red de distribución eléctrica **CA** (Corriente Alterna) de 50/60 Hz, radio AM y FM, Ultravioleta (en las frecuencias más altas de la luz visible), Infrarrojo (en las frecuencias más bajas de la luz visible) Rayos-X, y muchas otras.

Radio es el término utilizado para la porción del espectro electromagnético en la que las ondas pueden ser transmitidas aplicando corriente alterna a una antena. Esto abarca el rango de 30 kHz a 300 GHz, pero en el sentido más restringido del término, el límite superior de la frecuencia sería de 1 GHz, por encima del cual hablamos de microondas y ondas milimétricas.

Cuando hablamos de radio, la mayoría de la gente piensa en la radio FM, que usa una frecuencia de alrededor de 100 MHz. Entre la radio y el infrarrojo encontramos la región de las microondas –con frecuencias de 1 GHz a 300 GHz, y longitudes de onda de 30 cm a 1 mm.

El uso más popular de las microondas puede ser el horno de microondas que, de hecho, trabaja exactamente en la misma región que los estándares inalámbricos de los que estamos tratando.

Estas regiones caen dentro de las bandas abiertas para el uso general, sin requerir licencia.
Esta región es llamada ***banda ISM,*** por su sigla en inglés (*ISM Band),* Y en español ICM, que significa Industrial, Científica y Médica.

La mayoría de las otras regiones del espectro electromagnético están estrictamente controladas mediante licencias, siendo los valores de las licencias un factor económico muy significativo.

En muchos países, el derecho de uso de una porción del espectro se ha vendido a las compañías de telecomunicaciones en millones de dólares.
En la mayoría de los países, las bandas ISM han sido reservadas para el uso sin licencia, por lo tanto no se debe pagar para usarlas.

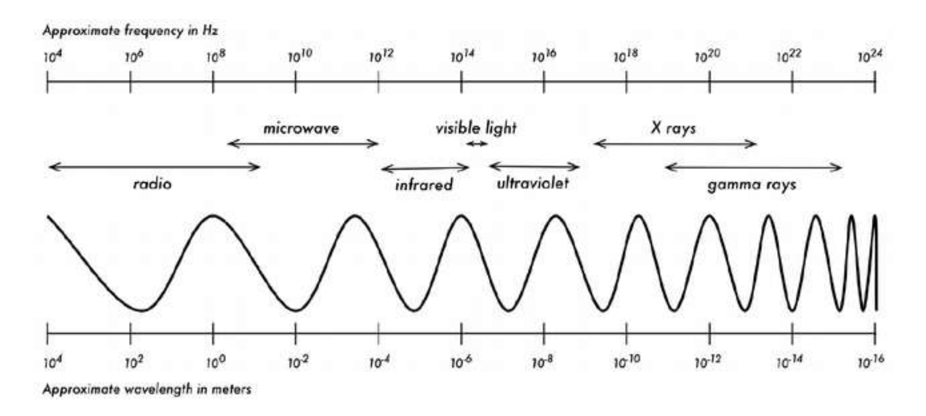


Figura FR 4: El espectro electromagnético

Las frecuencias más importantes para nosotros son las de 2 400 —2 495 MHz, usadas por los estándares 802.11b y 802.11g (correspondientes a longitudes de onda de alrededor de 12.5 cm), y las de 5.150 —5.850 GHz (correspondientes a longitudes de onda de alrededor de 5 a 6 cm), usadas por 802.11a. El estándar 802.11n puede trabajar en cualquiera de estas bandas.

Vea el capítulo ***Familia WiFi*** para una revisión de estándares y frecuencias. También puede encontrar más información sobre la parte de radio del espectro electromagnético en el capítulo ***Espectro Radioeléctrico***.

Ancho de banda

Un término que vamos a encontrar a menudo en la física de radio es ***ancho de banda***. El ancho de banda es simplemente una medida de rango de frecuencia. Si un dispositivo usa el rango de 2.40 GHz a 2.48 GHz, decimos que el ancho de banda sería 0.08 GHz (es decir 80 MHz).
Se puede ver fácilmente que el ancho de banda que definimos aquí esta muy relacionado con la cantidad de datos que se pueden trasmitir —a mayor cantidad de frecuencias disponibles, mayor cantidad de datos se pueden transmitir en un momento dado. El término ancho de banda es a menudo utilizado para algo que deberíamos más bien denominar tasa de transmisión de datos, por ejemplo "mi conexión a Internet tiene 1 Mbps de ancho de banda", lo que significa que ésta puede trasmitir datos a 1 megabit por segundo. Exactamente cuántos bits por segundo pueden transmitirse en un determinado rango de frecuencia dependerá de la modulación, la codificación y otras técnicas. Por ejemplo, 802.11g usa el mismo ancho de banda que 802.11b, pero puede contener más datos en esos mismos rangos de frecuencia y transmitir hasta 5 veces más bits por segundo. Otro ejemplo que hemos mencionado: se puede duplicar la tasa de transmisión de datos añadiendo un segundo enlace con una polarización perpendicular a un enlace de radio ya existente. En este caso, no se ha cambiado ni la frecuencia ni el ancho de banda, pero se ha duplicado la tasa de transmisión de datos.

Frecuencias y canales

Miremos un poco más de cerca cómo se utiliza la banda de 2.4 GHz en el estándar 802.11b. El espectro está dividido en partes iguales distribuidas sobre la banda en canales individuales. Note que los canales son de un ancho de 22 MHz, pero están separados sólo por 5 MHz.
Esto significa que los canales adyacentes se superponen, y pueden interferir unos con otros. Esto es representado visualmente en la figura FR 5.

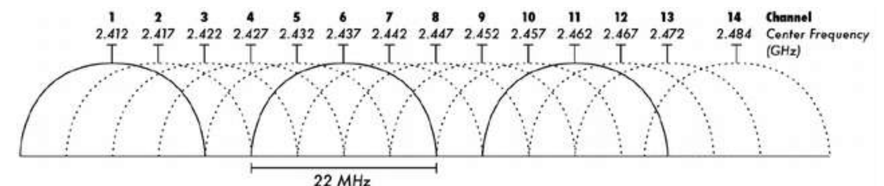


Figura FR 5: Canales y frecuencias centrales para 802.11b. Note que los canales 1, 6, y 11 no se superponen

Comportamiento de las ondas de radio

Hay algunas reglas simples que pueden ser de mucha ayuda cuando realizamos los primeros planes para una red inalámbrica:

- *Cuanto más larga la longitud de onda, mayor el alcance.*
- *Cuanto más larga la longitud de onda, mejor viaja a través y alrededor de obstáculos.*
- *Cuanto más corta la longitud de onda, puede transportar más datos.*

Todas estas reglas, simplificadas al máximo, son más fáciles de comprender con un ejemplo.

Las ondas más largas tienen mayor alcance

Las ondas con longitudes de onda más largas tienden a viajar más lejos que las que tienen longitudes de onda más cortas. Por ejemplo, las estaciones de radio AM tienen un alcance mayor que las de FM que usan frecuencias 100 veces mayores. Los transmisores de frecuencia más baja tienden a alcanzar distancias mucho más grandes que los de alta frecuencia, a la misma potencia.

Las ondas más largas rodean los obstáculos

Una onda en el agua que tiene 5 metros de longitud no va a ser afectada por un trozo de madera de 5 mm que esté flotando en el agua. Sin embargo, si la pieza de madera fuera de 50 metros (por ej. un barco), modificaría la trayectoria de la onda. La distancia que una onda puede viajar depende de la relación entre la longitud de onda de la misma y el tamaño de los obstáculos en su camino de propagación.

Es difícil visualizar las ondas "atravesando" objetos sólidos, pero ese es el caso de las ondas electromagnéticas. Cuanto más larga la longitud de onda (y por lo tanto una menor frecuencia) las ondas tienden a penetrar objetos mejor que las que tienen longitudes de onda más corta (y por consiguiente una frecuencia más alta). Por ejemplo, la radio FM (88-108 MHz) puede atravesar edificios y otros obstáculos fácilmente, mientras que las ondas más cortas (cómo los teléfonos GSM operando a 900 MHz ó 1 800 MHz) tienen más dificultades en penetrar edificios. Este efecto es debido, en parte, a los diferentes niveles de potencia utilizados por la radio FM y el GSM, pero también debido a las longitudes de onda más cortas de las señales GSM.

A frecuencias mucho más altas, la luz visible no pasa a través de una pared, o ni siquiera a través de una madera de 1 mm, como sabemos por experiencia.
Pero el metal va a detener cualquier tipo de onda electromagnética.

Las ondas más cortas pueden transmitir más datos
Cuanto más rápida sea la oscilación de la onda, mayor cantidad de información puede transportar: cada oscilación o ciclo podría ser utilizado para transportar un bit digital, un '0' o un '1', un 'sí' o un 'no'.
De esta manera la tasa de transmisión aumenta con el ancho de banda y puede aún ser mejorada por medio de técnicas de modulación y de acceso al medio avanzadas, omo OFDM (*Orthogonal Frequency-Division Multiplexing*) y MIMO (*Multiple Input, Multiple Output*).

El Principio de Huygens

Existe otro principio que puede ser aplicado a todos los tipos de ondas, y que es extremadamente útil para comprender la propagación de ondas de radio. Este principio es conocido como el ***Principio de Huygens***, en honor a Christiaan Huygens, matemático, físico y astrónomo holandés que vivió entre 1629 y 1695.

Imagine que toma una vara y la introduce verticalmente en un lago en calma, haciendo que el agua se agite y baile. Las ondas se alejarán de la vara —el lugar donde la introdujo en el agua—formando círculos.
Ahora bien, donde las partículas de agua están oscilando y bailando, las partículas vecinas harán lo mismo: desde cada punto de perturbación se origina una nueva onda circular. Esto es, de una forma simple, el principio de Huygens. Según *wikipedia.org*:

> "*El principio de Huygens es un método de análisis aplicado a los problemas de la propagación de ondas en el límite de campo lejano. Establece que cada punto de un frente de onda que avanza es, de hecho, el centro de una nueva perturbación y la fuente de un nuevo tren de ondas; y que esa onda avanzando como un todo, puede ser concebida como la suma de todas las ondas secundarias surgiendo de puntos en el medio ya atravesado. Esta visión de la propagación de ondas ayuda a comprender mejor la variedad de fenómenos de las ondas, tales como la difracción*".

Este principio se aplica tanto para las ondas de radio como para las ondas en el agua, para el sonido y para la luz –sólo que la longitud de onda de la luz es muy corta como para que los seres humanos podamos ver sus efectos directamente.
Este principio va a ayudarnos a comprender tanto la difracción, como las zonas de Fresnel, así como el hecho de que algunas veces las ondas doblan las esquinas más allá de la línea de vista.
Veamos entonces qué sucede con las ondas electromagnéticas cuando viajan.

Absorción

Cuando las ondas electromagnéticas atraviesan algún material, generalmente se debilitan o atenúan. La cantidad de potencia perdida va a depender de su frecuencia y, por supuesto, del material.
El vidrio de una ventana obviamente es transparente para la luz, mientras que el vidrio utilizado en los lentes de sol filtra una porción de la intensidad de la luz y bloquea la radiación ultravioleta.
A menudo se utiliza el coeficiente de absorción para describir el impacto de un material en la radiación. Para las microondas, los dos materiales más absorbentes son:

Metal. Los electrones pueden moverse libremente en los metales, y son capaces de oscilar y por lo tanto absorber la energía de una onda que los atraviesa.
Agua. Las microondas provocan que las moléculas de agua se agiten, capturando algo de la energía de las ondas.
En la práctica de redes inalámbricas, vamos a considerar el metal y el agua como absorbentes perfectos: no vamos a poder atravesarlos (aunque capas finas de agua dejan pasar parte de la potencia). Son a las microondas lo que una pared de ladrillo es a la luz.
Cuando hablamos del agua, tenemos que recordar que se encuentra en diferentes formas: lluvia, niebla, vapor y nubes bajas, y todas van a estar en el camino de los radioenlaces.
Tienen una gran influencia y en muchas circunstancias, un cambio en el clima puede hacer caer un radioenlace.
Cuando hablamos del metal, recuerde que puede hallarse en sitios inesperados: puede estar escondido en la paredes (por ejemplo, en rejillas de metal en el concreto), o puede haber capas delgadas en tipos modernos de vidrio (vidrio teñido o coloreado).

Por delgada que sea la capa de metal, puede ser suficiente para absorber una onda de radio).
Existen otros materiales que tienen un efecto más complejo en la absorción de las ondas de radio.
Para los árboles y la madera, la cantidad de absorción depende de la cantidad de agua que contienen. La madera vieja y seca es más o menos transparente, la madera fresca y húmeda va a absorber muchísimo.
Los plásticos, y materiales similares, generalmente no absorben mucha energía de radio, pero esto varía dependiendo de la frecuencia y el tipo de material.
Finalmente, hablemos de nosotros mismos: los humanos (como otros animales) estamos compuestos principalmente de agua. En lo que a redes inalámbricas se refiere, podemos ser descritos como grandes bolsas llenas de agua, con la misma fuerte absorción.
Orientar un punto de acceso en una oficina de forma que su señal deba pasar a través de mucha gente es un error grave cuando instalamos redes en oficinas. Lo mismo vale para *hot spots*, cafés, bibliotecas e instalaciones externas.

Reflexión

Al igual que la luz visible, las ondas de radio son reflejadas cuando entran en contacto con los materiales apropiados: para las ondas de radio, las principales fuentes de reflexión son el metal y las superficies de agua. Las reglas para la reflexión son bastante simples: el ángulo con el cual una onda incide en una superficie es el mismo ángulo con el cual es desviada.
Nótese que para las ondas de radio, una reja densa de metal actúa de igual forma que una superficie sólida, siempre que la distancia entre las barras sea pequeña en comparación con la longitud de onda.
A 2.4 GHz, una rejilla metálica con separación de 1 cm entre sus elementos va a actuar igual que una placa de metal.

A pesar de que las reglas de reflexión son bastante simples, las cosas pueden complicarse mucho cuando imaginamos el interior de una oficina con varios objetos pequeños de metal de formas variadas y complicadas.
Lo mismo sucede en las situaciones urbanas: mire alrededor en su ciudad e intente ubicar todos los objetos de metal.
Esto explica el por qué el ***efecto multitrayectoria (multipath)***, (es decir el que las señales lleguen al receptor a través de diferentes caminos, y por

consiguiente en tiempos diferentes), juega un rol tan importante en las redes inalámbricas.
La superficie del agua, con olas y encrespaduras que cambian su orientación todo el tiempo, hace que sea prácticamente imposible calcular precisamente la reflexión.

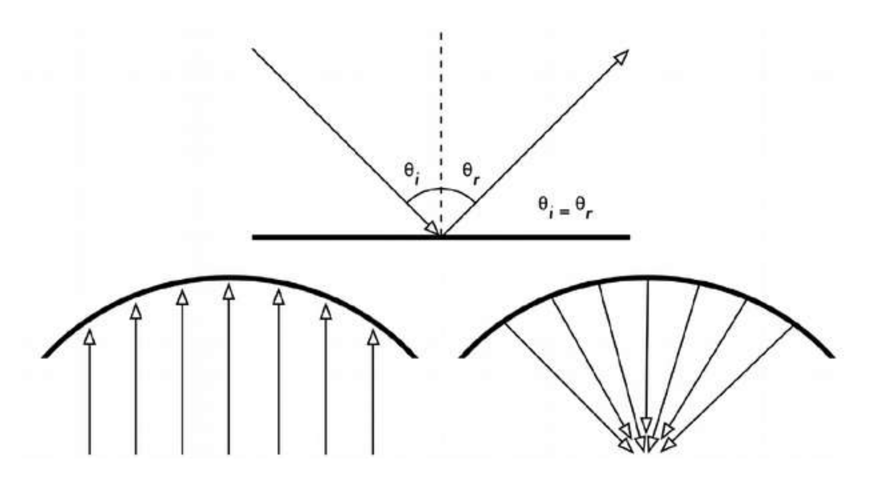


Figura FR 6: Reflexión de ondas de radio. El ángulo de incidencia es siempre igual al ángulo de reflexión. Una antena parabólica utiliza este efecto para concentrar las ondas de radio que caen sobre su superficie en un punto común

Debemos agregar que la polarización tiene un impacto: las ondas de diferente polarización en general van a ser reflejadas de forma diferente. Utilizamos la reflexión en ventaja nuestra en la construcción de las antenas: por ejemplo, colocando grandes parábolas detrás de nuestro transmisor/receptor para recoger las ondas de radio y concentrarlas en un punto.

Difracción

La difracción es el comportamiento de las ondas cuando, al incidir en un objeto, dan la impresión de doblarse. Es el efecto de “ondas doblando las esquinas”. Imagine una onda en el agua viajando en un frente de onda plano, tal como una ola llegándose a una playa oceánica.

Ahora interponemos en su camino una barrera sólida, como una cerca de madera, para bloquearla.
Luego practicamos una estrecha rendija en esa barrera, como una pequeña puerta.
Desde esta apertura se formará una onda circular, que alcanzará a puntos que están directamente al frente de la apertura, pero también a ambos lados de la misma.
Si miramos este frente de onda —y pudiera ser también una onda electromagnética—como un haz (una línea recta), sería difícil explicar cómo logra alcanzar puntos que están ocultos por una barrera.
Cuando lo modelamos como un frente de onda, el fenómeno tiene sentido.

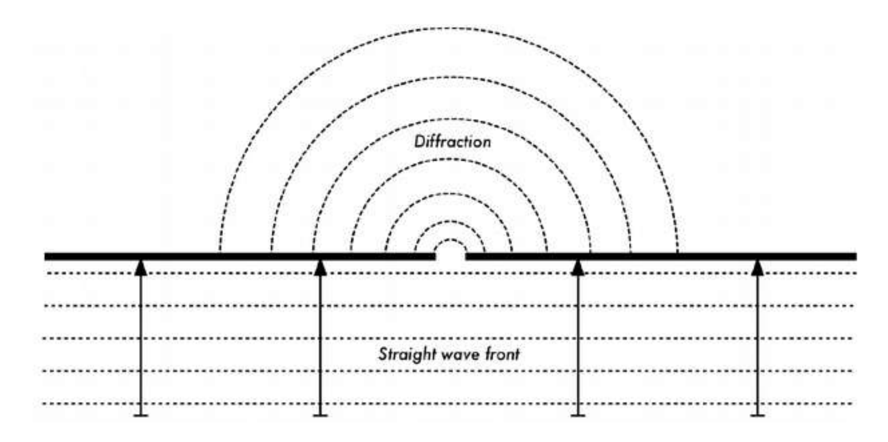


Figura FR 7: Difracción a través de una ranura estrecha

El Principio de Huygens provee un modelo para comprender este comportamiento.

Imagine que en un momento determinado, cada punto del frente de onda puede ser considerado como el punto de inicio de otra onda esférica.

Esta idea fue desarrollada más adelante por Fresnel, y si describe o no adecuadamente el fenómeno, todavía es tema de debate.
Pero para nuestros propósitos, el modelo de Huygens describe el efecto bastante bien.

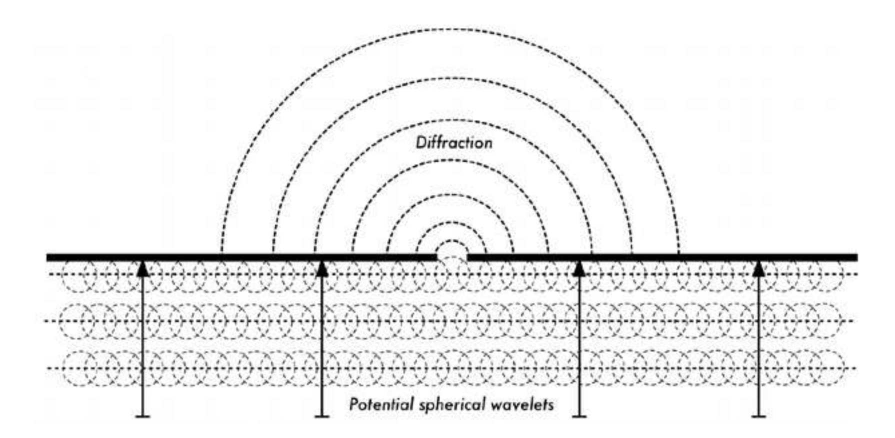


Figura FR 8: El Principio de Huygens

Es por medio del efecto de difracción, que las ondas van a "doblar" las esquinas, o van a atravesar una apertura en una barrera.
La longitud de onda de la luz visible es muy pequeña como para que los humanos puedan observar este efecto directamente.
Las microondas, con una longitud de onda de varios centímetros, muestran los efectos de la difracción cuando las ondas chocan contra paredes, picos de montañas y otros obstáculos. La obstrucción provoca que la onda cambie su dirección y doble las esquinas.

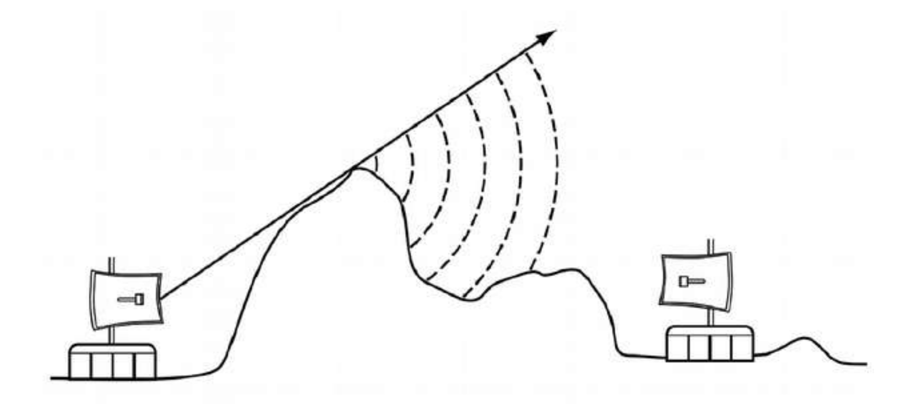


Figura FR 9: Difracción en la cima de una montaña

Tenga en cuenta que en la difracción se genera una pérdida de potencia: la potencia de la onda difractada es significativamente menor que el frente de onda que la provoca. Pero en algunas aplicaciones muy específicas, se puede aprovechar el efecto de difracción para rodear obstáculos.

Interferencia

La interferencia es uno de los términos y fenómenos más incomprendidos en redes inalámbricas.
La interferencia a menudo se lleva toda la culpa cuando somos demasiado perezosos para encontrar la raíz del problemas o cuando un ente regulador quiere clausurar la red de alguien por intereses económicos. ¿Por qué este malentendido?
Es más que todo porque las diferentes personas usan el mismo término para significados diferentes. Un físico y un ingeniero de comunicaciones van a usar el término "interferencia" para referirse a dos cosas distintas. El punto de vista del físico tendrá que ver con el comportamiento de las ondas. Para el ingeniero de comunicaciones es "...cualquier ruido que se atraviesa en el camino".
Los dos puntos de vista son relevantes para lo inalámbrico, y es importante conocer ambos y saber la diferencia. Comencemos con el punto de vista del físico:
Cuando se trabaja con ondas, uno más uno no es necesariamente dos: puede ser cero.

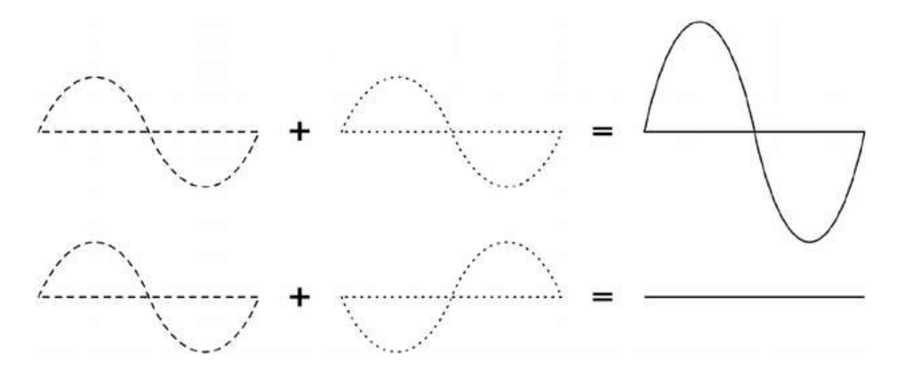


Figura FR 10: Interferencia constructiva y destructiva

Esto es sencillo de entender cuando dibujamos dos ondas senoidales y sumamos las amplitudes.

Cuando la diferencia de fase es 0 los picos coinciden, tenemos un resultado máximo (1 + 1 = 2).
Esto es denominado ***interferencia constructiva***.
Cuando la diferencia de fase es 180 grados, o $\lambda/2$, un pico coincide con un valle y obtenemos una completa aniquilación ((1 + (-)1 = 0) denominada ***interferencia destructiva***.
Puede probar esto creando dos olas circulares en el agua mediante dos varitas; verá que cuando dos olas se cruzan, hay áreas con picos de onda más grandes y otras que permanecen casi planas y en calma.
Para que los trenes de ondas se sumen o se cancelen perfectamente, tienen que tener exactamente la misma longitud de onda y una relación de fase fija. Se pueden observar ejemplos patentes de interferencia en acción mirando la forma en que las antenas están dispuestas en lo que se llama sistema de ***formación de haces (beamforming*** *arrays)*, con la finalidad de dar la mayor interferencia constructiva en la dirección donde se quiere la señal, y de interferencia destructiva (ausencia de señal) donde no se desea la señal.
Técnicamente, esto se logra por una combinación de dimensionamiento físico y control de los cambios de fase.

Simplificando, imagine que se tienen tres antenas y no queremos que la antena 3 reciba las señales de las antenas 1 y 2. Podríamos colocar la antena 3 en una posición tal que las señales provenientes de las antenas 1 y 2 se anulen entre sí.

Ahora, veamos otra manera en que se usa el término interferencia: en un sentido amplio, para cualquier disturbio de radio frecuencia, para cualquier ruido que nos afecte, de canales cercanos o de otros proveedores de servicio. De esta manera, cuando los constructores de redes inalámbricas hablan de interferencia, generalmente se refieren a todos los tipos de alteraciones generadas por otras redes y otras fuentes de microondas, sea que tengan exactamente la misma frecuencia y una relación de fase fija o no. La interferencia de este tipo es una de las fuentes principales de dificultades cuando se hacen enlaces inalámbricos, especialmente en ambientes urbanos o espacios cerrados (como una sala de conferencias) donde muchas redes compitiendo por el uso del espectro.
Pero el efecto de esta interferencia es a menudo exagerado: imagine, por ejemplo, que tiene que construir un enlace punto-a-punto que debe atravesar un área muy poblada del centro urbano antes de llegar a su objetivo en el otro extremo de la ciudad.

Un haz tan direccional atravesará la "jungla radioeléctrica urbana" sin ningún problema. Puede imaginarlo como un haz de luz rojo y otro verde que se cruzan en un ángulo de 90 grados: mientras que ambos haces van a superponerse en un área determinada, no se observará ningún impacto entre ellos.
Generalmente, la gestión del espectro y la coexistencia se han convertido en un asunto vital especialmente en ambientes interiores densos y en áreas urbanas.

Línea visual

El término ***línea visual*** *(también **línea de visión, línea de vista**)*, a menudo abreviada como ***LOS*** (por su sigla en inglés, *Line of Sight*), es fácil de comprender cuando hablamos acerca de la luz visible: si podemos ver un punto B desde un punto A donde estamos, tenemos línea visual. Dibuje simplemente una línea desde A a B, y si no hay nada en el camino, tenemos línea visual.
Las cosas se ponen un poco más complicadas cuando se trata de microondas. Recuerde que la mayoría de las características de propagación de las ondas electromagnéticas dependen de la longitud de onda. La luz tiene una longitud de onda de aproximadamente 0.5 micrómetros; las microondas usadas en las redes inalámbricas tienen una longitud de onda de unos pocos centímetros. Por consiguiente, los haces de microondas son más anchos –necesitan más espacio, por así decirlo.
Note que los haces de luz visibles también se ensanchan, y si los dejamos viajar lo suficiente, podemos ver los resultados a pesar de su pequeña longitud de onda.
Cuando apuntamos un láser bien enfocado a la luna, el haz se extenderá abarcando más de 100 metros de radio cuando alcance su superficie.
Puede observar este efecto por usted mismo/a utilizando un apuntador láser económico y un par de binoculares en una noche clara.
En lugar de apuntar a la luna, hágalo hacia una montaña distante o una estructura desocupada (como una cisterna de agua). El radio del haz va a incrementarse con la distancia. Esto se debe a la difracción.
La línea visual que necesitamos para tener una conexión inalámbrica óptima desde A hasta B no es solamente una línea delgada –su forma es más bien la de un tabaco, una elipsoide.
Su ancho puede ser descrito por medio del concepto de zonas de Fresnel explicado en la próxima sección.

También se encuentra la abreviatura ***NLOS*** para significar Ninguna Línea Visual (*Non Line Of Sight*), que es usada más que todo para describir y hacer propaganda de tecnologías que permiten el manejo de ondas que llegan al receptor a través de trayectorias múltiples (*multipath*) o difracción. No significa que el haz electromagnético único va a "doblar esquinas" (a menos que sea por difracción) o a pasar "a través de los obstáculos" mejor que con otras tecnologías. Por ejemplo, se podría llamar a la tecnología de los White Spaces tecnología NLOS (Ninguna Línea Visual) ya que sus frecuencias más bajas (longitudes de onda mayores) le permiten atravesar objetos y utilizar la difracción mucho mejor que las transmisiones comparables a 2.4 GHz o 5 GHz.

Para entender la zona de Fresnel

La teoría exacta de las zonas de Fresnel es algo complicada. Sin embargo, el concepto es fácilmente entendible: sabemos, por el principio de Huygens, que en cada punto de un frente de onda comienzan nuevas ondas esféricas. Sabemos que los haces de microondas se ensanchan a medida que se alejan de la antena.
También sabemos que las ondas de una frecuencia pueden interferir unas con otras. La teoría de la zona de Fresnel simplemente establece que entre dos puntos A y B la totalidad de la señal recibida en B incluye también zonas aledañas a la línea directa. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas y llegan al receptor por reflexión.

Como consecuencia, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos. Dondequiera que el desplazamiento de fase corresponde a media longitud de onda, se produce interferencia destructiva: las señales se anulan.
Tomando este enfoque, encontramos que cuando la trayectoria reflejada tiene una longitud menor que la mitad de la longitud de onda de la trayectoria directa, las reflexiones se suman a la señal recibida.

Por el contrario, cuando la longitud de la trayectoria reflejada excede a la de la trayectoria directa en más de la mitad de la longitud de onda, estos rayos van a disminuir la potencia recibida.

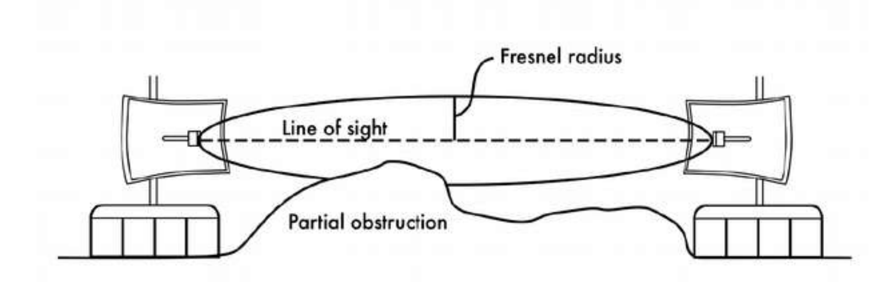


Figura FR 11: La zona de Fresnel está bloqueada parcialmente en este enlace aunque la línea visual (line of sight) no está obstruida

Tenga en cuenta que existen muchas zonas de Fresnel, pero a nosotros nos interesa principalmente la primera zona porque las contribuciones de la segunda son negativas. Las contribuciones de la tercera son de nuevo positivas, pero no se puede aprovechar sin la sanción de pasar por la segunda Zona de Fresnel.

Si la primera Zona de Fresnel está parcialmente bloqueada por un obstáculo, como un árbol o un edificio, la señal que llega al extremo lejano estará atenuada. Entonces, cuando planeamos enlaces inalámbricos, debemos asegurarnos de que esta zona va a estar libre de obstáculos. En la práctica, no es estrictamente necesario que la zona esté completamente despejada; para redes inalámbricas nos conformamos con despejar al menos el 60% del radio de la primera zona de Fresnel.

$$r = 17.31\sqrt{\left(\frac{(d_1 * d_2)}{(f * d)}\right)}$$

donde **r** es el radio de la primera zona en metros, **d1** y **d2** son las distancias desde el obstáculo a los extremos del enlace en metros, **d** es la distancia total del enlace en metros, y **f** es la frecuencia en MHz.
El radio de la primera zona de Fresnel puede también calcularse directamente a partir de la longitud de onda de esta manera:

$$r = \sqrt{\left(\frac{\lambda * d_1 * d_2}{d}\right)}$$

con todas las variables en metros

Es aparente que el valor máximo de la primera zona de Fresnel ocurre exactamente en la mitad de la trayectoria y su valor puede obtenerse haciendo d_1=d_2=d/2 en las fórmula precedentes.
Note que las fórmulas le dan el radio de la zona pero no la altura sobre el terreno. Para calcular la altura sobre el terreno, debe sustraer este resultado de una línea trazada directamente entre la cima de las dos torres (o a la altura donde estén las antenas en la torre).
Por ejemplo, calculemos el tamaño de la primera zona de Fresnel en el medio de un enlace de 2 km, transmitiendo a 2.437 GHz (802.11b canal 6):

$$r=17.31\sqrt{[\frac{(1000*1000)}{(2437*2000)}]}$$

$$r=17.31\sqrt{(\frac{1000000}{4874000})}$$

$$r = 7.84 \text{ metros}$$

Suponiendo que ambas torres tienen 10 metros de altura, la primera zona de Fresnel va a pasar justo a 2.16 metros sobre el nivel del suelo en el medio del enlace. Pero, ¿cuán alta puede ser una estructura en este punto para no bloquear más del 60% de la primera zona?

$$R = 0.6 * 7.84 \text{ metros}$$
$$r = 4.70 \text{ metros}$$

Restando el resultado de los 10 metros, podemos ver que una estructura de 5.30 metros de alto en el centro del enlace bloquearía hasta el 40 % de la primera zona de Fresnel.
Esto es normalmente aceptable, pero en el caso de que hubiera una estructura más alta, habría que levantar más nuestras antenas, o cambiar la dirección del enlace para evitar el obstáculo.

Potencia

Cualquier onda electromagnética contiene energía, ~~lo~~ podemos sentir cuando disfrutamos (o sufrimos) del calor del sol.

La cantidad de energía dividida por el tiempo durante el cual la medimos se llama potencia. La potencia ***P*** se mide en W (vatios) y es de una importancia clave para lograr que los enlaces inalámbricos funcionen: se necesita cierto mínimo de potencia para que el receptor detecte adecuadamente la señal.
Vamos a volver con más detalles sobre la potencia de transmisión, pérdidas, ganancia y sensibilidad del radio en el capítulo sobre *Antenas y Lineas de Transmisión*.
Ahora vamos a discutir brevemente cómo se define y calcula la potencia **P**.
El campo eléctrico se mide en V/m (diferencia de potencial por metro); la potencia contenida en él es proporcional al cuadrado del campo eléctrico
$P \sim E^2$

En la práctica, medimos la potencia en vatios por medio de algún tipo de receptor, por ej. una antena y un voltímetro, un medidor de potencia, un osciloscopio, un analizador de espectro, o inclusive una tarjeta inalámbrica y una computadora portátil. La potencia también se puede calcular directamente como el cuadrado de la señal en voltios dividido por el valor de la resistencia eléctrica en ohmios.

Cálculo en dB

Sin duda la técnica más importante para calcular la potencia es el cálculo en *decibelios* (*dB*). No hay física nueva en esto, es solamente un método conveniente que hace que los cálculos sean muy simples.
El decibelio es una unidad sin dimensión, esto es, define la relación entre dos medidas de potencia. Se define como:
$dB = 10 * Log (P_1 / P_0)$

donde $\mathbf{P_1}$ **and** $\mathbf{P_0}$ pueden ser dos valores cualesquiera que queramos comparar. Normalmente, en nuestro caso, se tratará de potencia.
¿Por qué es tan práctico el uso de decibelios? Muchos fenómenos de la naturaleza se comportan de una manera que llamamos exponencial. Por ejemplo, el oído humano percibe un sonido dos veces más intenso que otro si el primero tiene diez veces la potencia del segundo.

Otro ejemplo, muy relacionado con nuestro campo de interés, es el de la absorción.

Imaginemos una pared en el camino de nuestro enlace inalámbrico, y cada metro de esa pared absorbe la mitad de la señal disponible.
El resultado va a ser:

0 metros = 1 (señal completa)
1 metro = 1/2
2 metros = 1/4
3 metros = 1/8
4 metros = 1/16
n metros = $1/2^n = 2^{-n}$

Este es el comportamiento exponencial.
El empleo de los logaritmos facilita las operaciones matemáticas. Elevar a la enésima potencia es sustituido por multiplicar por n, y la multiplicación de dos cantidades es sustituida por la suma de sus logaritmos.

He aquí algunos valores que es importante recordar:

+3 dB = doble potencia
-3 dB = mitad de la potencia
+10dB=orden de magnitud (10 veces la potencia)
-10 dB = un décimo de la potencia

Además de los dB adimensionales, hay cierto número de definiciones relacionadas que están basadas en una referencia P_0 fija. Las más relevantes para nosotros son:

dBm relativo a P_0 *= 1 mW*
dBi relativo a una antena isotrópica ideal

Una **antena isotrópica** es una antena hipotética que distribuye uniformemente la potencia en todas direcciones. La antena que más se aproxima a este concepto es la dipolo, pero una antena isotrópica perfecta no puede ser construida en la realidad.
El modelo isotrópico es útil para describir la ganancia de potencia relativa de una antena real.

Otra forma común (aunque menos conveniente) de expresar la potencia es en milivatios (*milliwatts*: mW).

A continuación algunas equivalencias de niveles de potencia expresadas en mW y dBm:

1 mW = 0 dBm
2 mW = 3 dBm
100 mW = 20 dBm
1 W = 30 dBm

Para más detalles sobre dB vaya a la conferencia relacionada del *Wireless Training kit*:

http://wtkit.org/groups/wtkit/wiki/c3bc2/WTKit_spanish.html

La física en el mundo real

No se preocupe si los conceptos de este capítulo le parecen apabullantes. Entender cómo las ondas de radio se propagan e interactúan con el medio ambiente es un campo de estudio complejo en sí mismo. La mayoría de la gente encuentra difícil la comprensión de fenómenos que no puede ver con sus propios ojos.
En este punto, esperamos que el/la lector/a pueda comprender que las ondas de radio no viajan solamente por un camino recto predecible. Para construir redes de comunicación confiables, se debe ser capaz de calcular cuánta potencia se necesita para cruzar una distancia dada, y predecir cómo van a viajar las ondas a lo largo del camino.

2. TELECOMUNICACIONES BÁSICAS

El propósito de cualquier sistema de telecomunicaciones es el de transferir i*nformación* desde un emisor a un receptor por medio de un c*anal* de comunicación.
La información es transportada en una *señal*, que es una cierta cantidad física que cambia en el tiempo.

La señal puede ser un voltaje proporcional a la amplitud de la voz, como en un simple teléfono, una secuencia de impulsos de luz en una fibra óptica o una onda radioeléctrica irradiada por una antena.

Para señales analógicas estas variaciones son directamente proporcionales a alguna variable física, como el sonido, luz, temperatura, velocidad del viento, etc. La información también puede transmitirse por señales binarias digitales que tendrán sólo dos valores, un uno digital y un cero digital. Cualquier señal analógica puede transformarse en digital por medio de un muestreo apropiado y seguida de codificación. La frecuencia de muestreo debe ser por lo menos el doble de la máxima frecuencia presente en la señal para preservar toda la información contenida. Las señales aleatorias son aquellas impredecibles que sólo pueden describirse por medios estadísticos.
El ruido es una señal aleatoria típica descrita por su potencia promedio y la distribución estadística de la potencia sobre las frecuencia. Una señal se caracteriza por su comportamiento en el tiempo o por sus componentes de frecuencia, lo cual constituye su espectro. En la figura TB 1 tenemos ejemplos de señales.

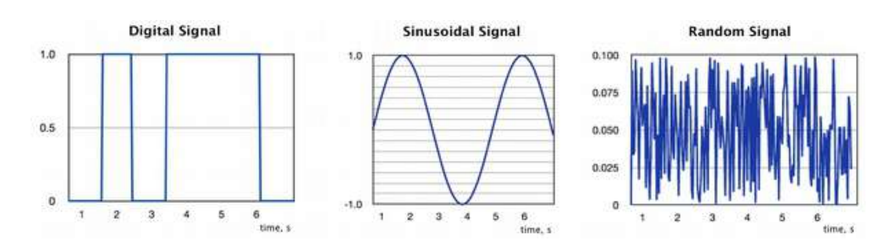


Figura TB 1: Ejemplos de señales

Cualquier señal periódica tiene muchas componentes sinusoidales, todas ellas múltiplos de la frecuencia fundamental que es el inverso del período de

la señal. Así, una señal se caracteriza bien por un gráfico de su amplitud en el tiempo, lo que se llama una forma de onda, o por un gráfico de las amplitudes de sus componentes de frecuencia, llamado espectro.

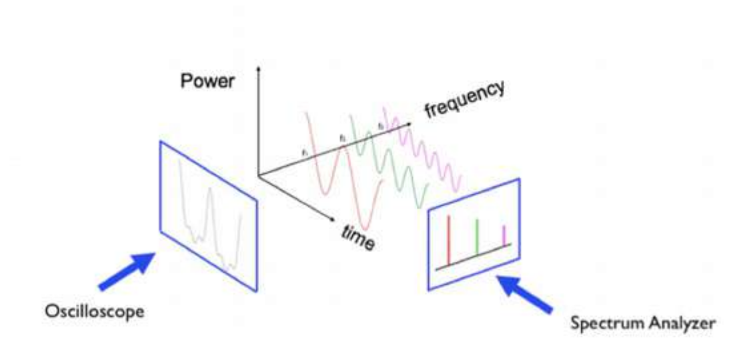


Figura TB 2: Formas de onda, espectro y filtros

La Figura TB 2 muestra cómo la misma señal puede verse desde dos perspectivas diferentes. La forma de onda se puede visualizar a través de un instrumento llamado Osciloscopio, mientras que el espectro puede visualizarse en un Analizador de Espectro.
La distribución espectral ofrece información importante sobre la señal y permite la comprensión intuitiva del concepto de filtrado de las señales eléctricas. En los ejemplos vistos, la señal está formada por la superposición de tres componentes sinusoidales de frecuencia f_1, f_2 y f_3. Si a esta señal la pasamos a través de un dispositivo que remueva f_2 y f_3, el resultado es una simple sinusoide a la frecuencia f_1.
Esta operación se llama "**Filtro Paso Bajo**" porque remueve las frecuencias altas. Por el contrario podemos aplicarle a la señal un "**Filtro Paso Alto**", un dispositivo que remueve f_1 y f_2, dejando sólo la sinusoide a la frecuencia f_3.
Hay otras combinaciones posibles que dan origen a una variedad de filtros. No existe un dispositivo físico capaz de transmitir las infinitas frecuencias del espectro radioeléctrico, así que cada dispositivo siempre ejercerá **algún** filtrado a la señal que lo atraviese.
Mientras viaja por el canal de comunicación, la señal puede sufrir *interferencias* causadas por otras señales y también verse afectada por el *ruido* eléctrico siempre presente en todo componente eléctrico u óptico.
La interferencia *intra-canal* se origina en el mismo canal de la señal.

La interferencia *co-canal* se debe a las imperfecciones de los filtros que dejarán entrar señales desde otros canales adyacentes.
En consecuencia, la señal recibida será siempre una réplica distorsionada de la señal que se transmite, a partir de la cual se debe extraer la información original utilizando medios apropiados para combatir los efectos de la interferencia y el ruido. Además, la señal recibida sufrirá *atenuación* y *retraso* que aumentarán con la distancia entre el transmisor y el receptor.

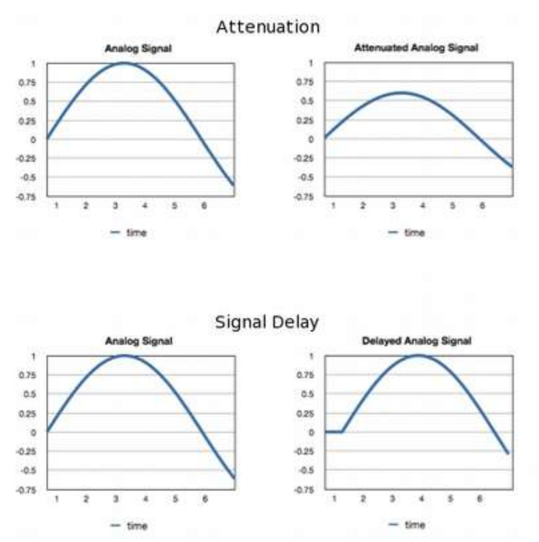


Figura TB 3: Atenuación y retardo

A pesar de que es relativamente sencillo recuperar la amplitud de la señal por medio de un *amplificador* eléctrico, los componentes de éste añadirán ruido adicional a la señal de tal manera que a distancias grandes donde la señal recibida es débil, el amplificador va a producir una señal tan contaminada por el ruido que la información transmitida originalmente no será ya recuperable.
Una forma de enfrentar este problema consiste en convertir la variable continua que transporta la información en una secuencia de *símbolos* sencillos que son más fáciles de reconocer incluso a grandes distancias. Por ejemplo, la bandera de un barco es una manera conveniente para distinguir la nacionalidad del mismo incluso a distancias tan grandes que no permiten la lectura de las letras en el casco.
Esta técnica se ha extendido para transmitir mensajes de todo tipo

asignando diferentes posiciones de las banderas a cada letra del alfabeto en una forma precursora de telecomunicaciones por medio de señales *digitales* , también llamadas *numéricas*. La limitación de este método es obvia: para distinguir entre los más o menos 26 símbolos de cada letra del alfabeto, uno tiene que estar bastante cerca del barco que comunica.
Por otra parte, si codificamos cada letra del alfabeto en una secuencia de sólo dos símbolos, como por ejemplo los puntos y rayas del sistema telegráfico, estos pueden distinguirse desde distancias más grandes.

El proceso por el cual se transforma una señal analógica continua en una digital discontinua se llama Conversión Analógica a Digital (*Analog to Digital Conversion:* ADC) y viceversa, debemos tener un Convertidor Digital a Analógico (DAC) en el extremo receptor para recuperar la información original. Esta es la razón por la cual la mayoría de los sistemas de telecomunicación modernos usan señales digitales binarias para transmitir todo tipo de información de una manera más robusta.
El receptor debe distinguir solamente entre dos símbolos posibles, o en otras palabras, entre dos posibles valores del bit (***bi***nary digi***t***: dígito binario) recibido. Por ejemplo, el CD ha reemplazado el disco de vinilo y la televisión analógica se está reemplazado por la digital. Las señales digitales pueden usar menos ancho de banda, como se ejemplifica en el "***dividendo digital***" que hoy en día se aprovecha en muchos países y que consiste en el ancho de banda que ha quedado libre gracias al paso de transmisión analógica a digital en la radiodifusión de TV. A pesar de que el proceso de convertir un sistema de información analógico en uno digital comporta siempre alguna pérdida de información, podemos diseñar el sistema para minimizar esa pérdida.





Figura TB 4: Imagen insuficientemente muestreada

Por ejemplo, en una cámara digital podemos escoger el número de bits usados para grabar la imagen. Cuanto mayor sea el número de bits (proporcional al número de megapixeles), mejor será imagen, pero se necesitará más memoria y más tiempo para transmitirla. Así es como la mayoría de los sistemas de comunicación modernos trabajan con señales digitales a pesar de que la variable original que queremos transmitir sea analógica, como la voz. Se puede demostrar que cualquier señal analógica puede reconstruirse a partir de sus muestras discretas si la frecuencia de muestreo es por lo menos el doble de la frecuencia más alta contenida en la señal.

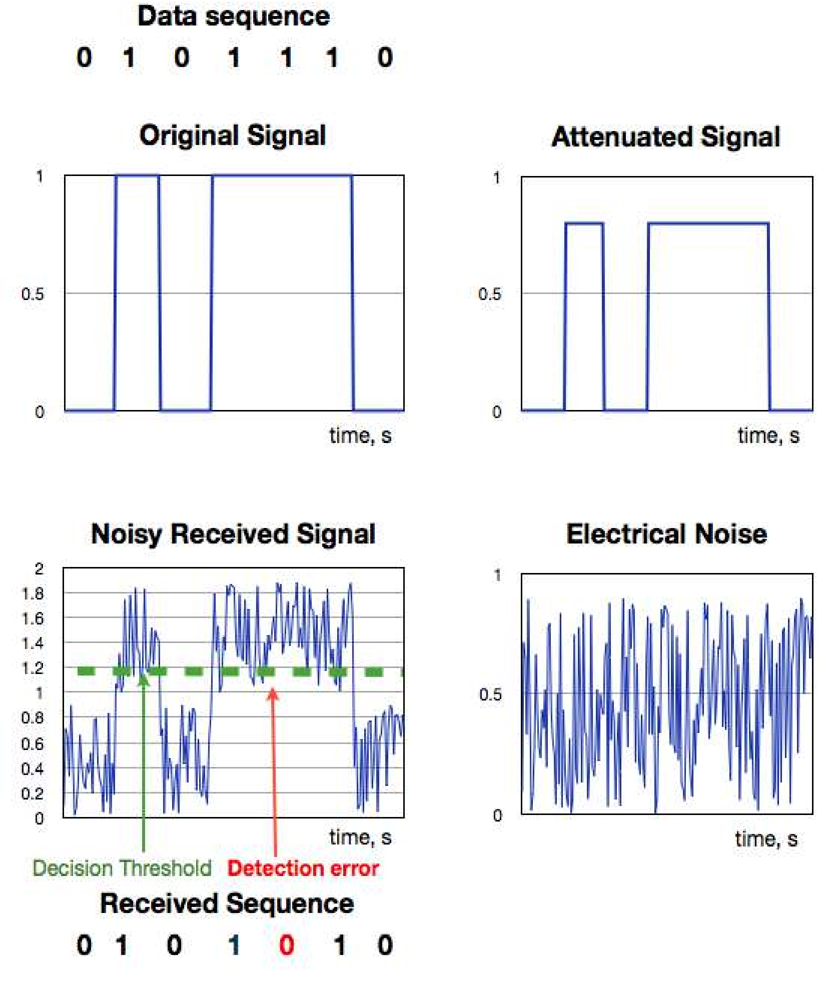


Figura TB 5: Detección de una señal ruidosa

Posteriormente cada muestra es codificada en tantos bits como sea necesario para lograr la precisión deseada.

Estos bits pueden ahora almacenarse o transmitirse de manera eficiente puesto que para recuperar la información necesitamos distinguir solamente entre dos estados y no entre los infinitos detalles de una señal analógica.

Esto se muestra en la Figura TB 5, donde los datos originales consisten en la secuencia 0 1 0 1 1 1 0. Los 0 se representan como 0 voltios y los 1 como 1 V. A medida que la señal se mueve hacia el receptor, su amplitud disminuirá. Este efecto se llama "atenuación" y se muestra en la figura. Asimismo, también habrá un retraso a medida que la seña se mueve desde el transmisor al receptor. La variabilidad en el retraso de la señal recibida se llama ***fluctuación de retardo*** (*jitter*).

Si la atenuación, el ruido y la fluctuación de retardo (o su combinación) son severas, pueden generar errores de detección. Se puede usar un amplificador para solucionar la atenuación, pero el ruido eléctrico siempre presente en el sistema se sumará a la señal recibida.

La señal ruidosa que se recibe es por lo tanto muy diferente a la señal original, pero en un sistema digital podemos recuperar la información contenida muestreando la señal recibida en el tiempo correcto y comparando el valor que tiene en el tiempo del muestreo con un umbral de voltaje apropiado.

Los errores de transmisión también ocurren si el período de muestreo de la señal es diferente del de los datos originales (diferencia en la frecuencia de reloj) o si el reloj recibido no es suficientemente estable (fluctúa).
Cualquier sistema físico tendrá un límite superior en cuanto a las frecuencias que va a transmitir con fidelidad (el ancho de banda del sistema). El bloqueo de las frecuencias altas cuando la señal atraviesa el canal se manifiesta en la incapacidad de responder a las caídas y subidas abruptas de tensión, con lo que la señal recibida es una versión "redondeada" de la de entrada.
Por consiguiente, debemos garantizar que cada elemento del sistema tenga un ancho de banda suficiente para manejar la señal. Por otra parte, cuanto mayor sea el ancho de banda del sistema receptor, mayor será la cantidad de ruido que afectará la señal recibida.

Modulación

La robustez de la señal digital también se ejemplifica por el hecho de que fue escogida para las primeras pruebas de radio transmisión.
Marconi había demostrado la factibilidad de transmisiones de larga distancia, pero pronto se dio cuenta de que existía la necesidad de compartir el medio con diferentes usuarios. Esto se logró asignando diferentes frecuencias *portadoras* que eran *moduladas* por el *mensaje* de cada usuario.
La *modulación* es una estrategia para modificar la *amplitud*, la *frecuencia* o la *fase* de la portadora de acuerdo con la información que uno quiere transmitir. La información original se recupera en el destino por medio de la correspondiente demodulación de la señal recibida.

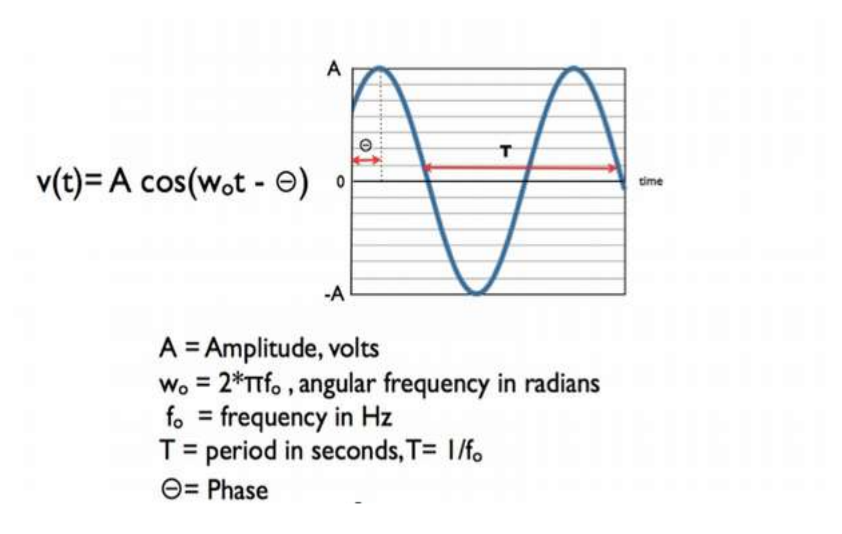


Figura TB 6: Señal Portadora Sinusoidal

La Figura TB 6 muestra una portadora con una Amplitud A, una fase θ, y una frecuencia fo que es la recíproca del período T.

La combinación de diferentes estrategias de modulación ha producido una plétora de técnicas de modulación dependiendo de cuál aspecto se quiere optimizar: robustez al ruido; cantidad de información transmitida por segundo (capacidad del enlace en bits/segundo) o eficiencia espectral (número de bits/s por Hertz).

Por ejemplo, la Modulación Binaria por Desplazamiento de Fase Binary Phase Shift Keying: BPSK es una técnica muy robusta pero que transmite sólo un bit por símbolo, mientras que la Modulación de Amplitud en Cuadratura (256 QAM-Quadrature Amplitude Modulation-) transporta 8 bits por símbolo, multiplicando por un factor de 8 la cantidad de información transmitida por segundo, pero para distinguir correctamente entre los 256 símbolos transmitidos, la señal recibida debe ser muy fuerte en comparación con el ruido (se necesita una relación S/R señal/ruido muy grande).
La medida de la calidad en transmisión digital se expresa mediante el BER (Bit Error Rate) o Relación (Bits Erróneos)/(total de bits recibidos) que es la fracción de bits recibidos erróneamente descodificados. Los valores típicos de BER oscilan entre 10-3 y 10-9. La modulación también nos permite escoger cuál rango de frecuencia queremos emplear para una transmisión dada. No todas las frecuencias son iguales y la elección de la frecuencia de la portadora está determinada por limitaciones legales, comerciales y técnicas.

Multiplexación y duplexación

En general, la compartición de un canal entre diferentes usuarios se llama *multiplexación.* Esto se muestra en la Figura TB 7.

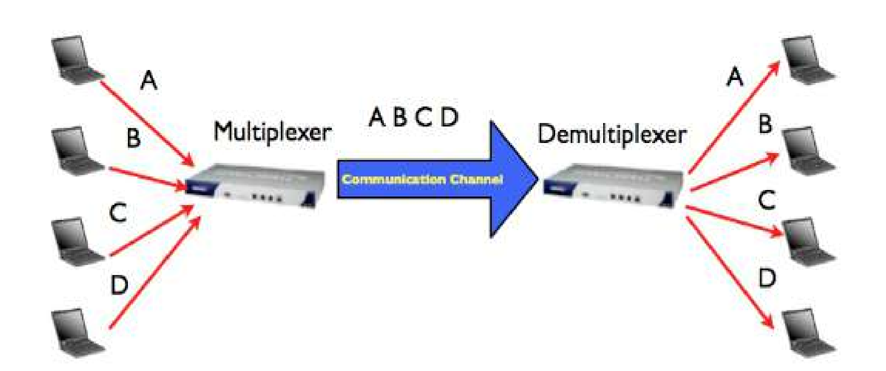
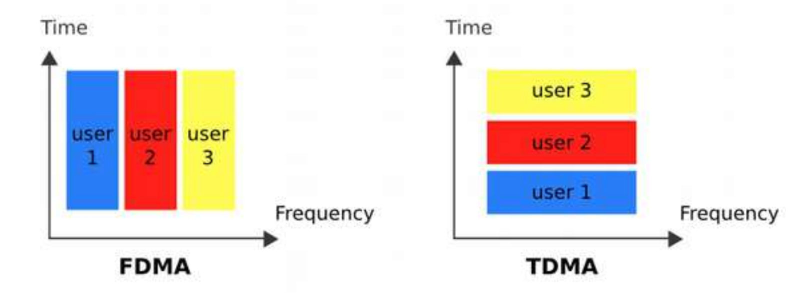


Figura TB 7: Multiplexación

Asignar diferentes frecuencias portadoras a diferentes usuarios se conoce como Acceso Múltiple por División de Frecuencia o FDMA por su sigla en inglés (Frequency Division Multiple Access).

Una técnica alternativa consiste en asignar diferentes franjas de tiempo a diferentes usuarios en lo que se llama Acceso Múltiple por División de Tiempo o TDMA por su sigla en inglés (Time Division Multiple Access), o incluso diferentes códigos: CDMA Acceso Múltiple por División de Código o CDMA por su sigla en inglés (Code Division Multiple Access), donde los diferentes usuarios son reconocidos en el receptor por un código matemático particular que se les asigna. Vea la Figura TB 8.
Cuando se usan dos o más antenas simultáneamente se puede aprovechar la diferencia en el desvanecimiento (fading) debida a las diferentes trayectorias hacia el receptor para establecer una diferencia entre usuarios en lo que se conoce como Acceso Múltiple por División de Espacio o SDMA por su sigla en inglés (Space Division Multiple Access), una técnica empleada en los sistemas MIMO (Múltiple Input, Múltiple Output), que se han hecho muy populares últimamente.

Medium sharing techniques



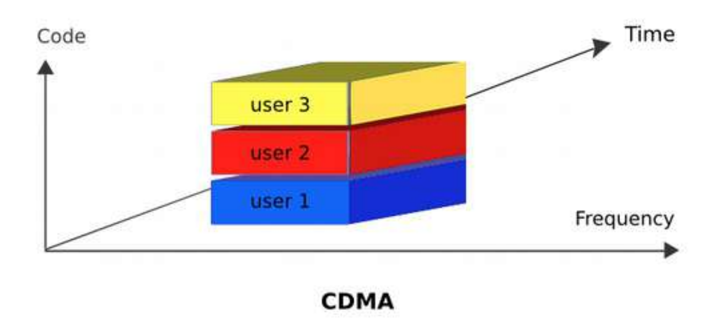


Figura TB 8: Técnicas de compartición del medio

Muchos sistemas de comunicación transmiten información en ambas direcciones, por ejemplo, desde la estación base al subscriptor en lo que se llama un ***enlace descendente*** *(downlink)*, y desde el subscriptor a la estación base en lo que se llama ***enlace ascendente*** *(uplink)*.
Para lograr esto, el canal debe ser compartido entre las dos direcciones dando lugar a FDD *-Frequency Division Duplexing-* y TDD *-Time Division Duplexing.*

Conclusiones

El sistema de comunicación debe superar el ruido y la interferencia para entregar una réplica adecuada de la señal enviada al receptor.

La capacidad del canal de comunicación en bits/segundo es proporcional al ancho de banda en Hz y al logaritmo de la relación Señal/Ruido.

La modulación se usa para adaptar la señal al canal y para permitir que varias señales compartan el mismo canal. Hay estrategias de modulación avanzadas que permiten una tasa de transmisión de datos más alta pero que también requieren de una relación Señal/Ruido más alta.

El canal puede ser compartido por varios usuarios que ocupan diferentes frecuencias, diferentes intervalos de tiempo, diferentes códigos o aprovechando las diferentes características de propagación en lo que se conoce como multiplexación espacial.

Para más información y diapositivas sobre este tópico, visite:

http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html

3. LICENCIAS Y REGULACIONES

Hay un número de áreas donde las leyes nacionales e internacionales pueden afectar su habilidad para instalar redes inalámbricas.
Puesto que estas reglas varían de país en país es imposible dar una visión general de cuáles son las regulaciones aplicables en su país.
Hay que hacer notar también que existe una gran diferencia en las leyes existentes y su aplicación en la práctica. En otras palabras, hay países donde en teoría usar el espectro de 2.4 GHz/5 GHz para instalaciones inalámbricas exteriores requiere de licencia previa, sin embargo, en la práctica la gente que los usa sin cumplir con este requisito no sufre las consecuencias. Como regla general si otra gente está instalando redes semejantes a la que usted quiere instalar, contáctelos y averigüe cuáles problemas legales pueden haber encontrado. Si hay este tipo de redes instaladas profusamente en su país probablemente no necesite preocuparse mucho entonces. Por otra parte, se aconseja siempre buscar consejos locales de parte de los distribuidores de hardware, expertos inalámbricos u otros que hayan instalado anteriormente antes de dedicarle tiempo y recursos a construir una red inalámbrica. Cualquier cosa que haga, es importante que tome en cuenta las leyes y regulaciones locales.

Ejemplos de regulaciones relevantes

Cada país puede tener reglas diferentes y cada situación puede encontrar varios tipos de regulaciones. Las áreas donde las regulaciones pueden ser relevantes incluyen licencias para usar radiofrecuencias específicas, reglas sobre el derecho de instalación de torres para antenas, la potencia máxima permitida y reglas sobre licencias de telecomunicación que limitan su habilidad para darle acceso de Internet a otros. Los tipos de problemas legales que pueden valer (o no) la pena de considerar cuando se planea una red inalámbrica incluyen:

- Licencia del uso del espectro
- Licencias para Proveedores de Servicio de Internet (ISP) o de Telecomunicaciones
- Permisos para torres de antenas
- Límites de potencia de transmisión y ganancia de antenas
- Certificación de equipos
- Condiciones de uso del ISP (*Internet Service Provider*)

Licencia del uso del Espectro

La mayor parte de los países considera el espectro de RF como una propiedad del estado. El espectro de RF es un recurso nacional como lo es el agua, la tierra, el gas y los minerales. A diferencia de estos, sin embargo, el espectro de RF es reutilizable. El propósito de la gerencia del espectro es la mitigación de la contaminación del espectro de radio y la optimización de los beneficios del espectro radioeléctrico utilizable.

En la primera frase del reglamento de la Unión Internacional de Telecomunicaciones (UIT), se reconocen "los derechos soberanos de cada Estado para regular sus telecomunicaciones". La gerencia efectiva del espectro requiere de la regulación a nivel nacional, regional y global.

El licenciamiento es una manera organizada de regular quién, cuándo, dónde y cómo se utiliza el recurso del espectro. En la banda de 2.4 GHz se permite el uso de redes inalámbricas sin necesidad de licencia.

En junio de 2003 la UIT puso a disposición la banda de 5 GHz para el uso de tecnología exenta de licencia. La banda de 900 MHz, sin licencia en los EEUU, se utiliza en Europa Occidental y en algunos países en desarrollo para teléfonos GSM. Cada país tiene el derecho soberano de regular sus telecomunicaciones y de interpretar las Regulaciones de Radio internacionales. Los gobiernos definen las reglas y las condiciones del uso de la frecuencia. (De Wikipedia: "Spectrum Management")

Las mayor parte de las tecnologías aquí descritas usan un segmento del espectro exento de licencia llamado bandas de radio para uso Industrial Científico y Médico (bandas ISM). Las radiofrecuencias en las bandas ISM se han usado para comunicaciones, pero pueden sufrir interferencias proveniente de otros dispositivos que no sean de comunicaciones.

Las bandas ISM están fijadas por el UIT-R (Sector de Radiocomunicaciones de la UIT) a 2.4 y 5 GHz. Sin embargo, cómo usa cada país las bandas asignadas en estas secciones puede diferir debido a las variaciones en las regulaciones nacionales.

Los dispositivos de comunicaciones que usan las bandas ISM deben tolerar cualquier interferencia proveniente bien sea de equipos de comunicaciones o de otra índole. El mecanismo de acceso al medio está diseñado para diferir la comunicación cuando el medio está ocupado.

En los EEUU, la FCC (*Federal Communications Commission*) autorizó el uso sin licencia de equipos de telecomunicaciones de espectro esparcido en las bandas ISM en un reglamento del 9 de mayo de 1985. Muchos otros países posteriormente adoptaron regulaciones semejantes.

Licencias para Proveedores de Servicios de Internet (ISP) y de Telecomunicaciones

En algunos países se necesita una licencia de ISP antes de implementar cualquier estructura para compartir redes en zonas públicas. En otros países se necesita sólo para redes de uso comercial.

Permisos de torres para antenas

Cuando se implementan redes exteriores de largo alcance se hace necesario a menudo construir una torre para la antena. En muchos países se necesitan permisos especiales si estas torres exceden de determinada altura.

Límites a la potencia de transmisión

Cuando se establecen límites para la potencia de transmisión los entes reguladores usan a menudo la Potencia Isotrópica Radiada Equivalente o PIRE (*Equivalent Isotropically Radiated Power, EIRP*), porque esa es la potencia efectivamente irradiada por la antena en su dirección preferente. La potencia de salida de los dispositivos también puede estar sujeta a límites. Para dar un ejemplo, la FCC establece un valor máximo de la potencia de transmisión del radio. Adicionalmente, establece valores máximos de la ganancia de la antena que son diferentes en las instalaciones punto a multipunto (PtMP) de las correspondientes instalaciones punto a punto (PtPt).

Cuando se usa una antena omnidireccional la FCC considera automáticamente el enlace como PtMP. En la configuración de un enlace PtMP a 2.4 GHz, la FCC limita la PIRE a 4 vatios y la potencia máxima del elemento radiante intencional a 1 vatio.

Las cosas se complican más en la banda de 5 GHz. La banda de radio UU-NII (*Unlicensed National Information Infrastructure*) es parte del espectro de radiofrecuencia usado por los dispositivos IEEE-802.11a y por muchos ISP inalámbricos. Opera en tres rangos:

- U-NII Baja (U-NII-1): 5.15-5.25 GHz. Las regulaciones estipulan el uso de una antena integrada. La potencia está limitada a 50 mW.
- U-NII Media (U-NII-2): 5.25-5.35 GHz. Las regulaciones permiten una antena instalable por el usuario sujeta a Selección Dinámica de Frecuencia o DFS en inglés (Dynamic Frequency Selection), para evitación interferencia con radar. Potencia limitada a 250 mW.

- U-NII Global: 5.47-5.725 GHz. Tanto para el uso interno como el de exteriores sujeto a Selección de Frecuencia Dinámica (DFS). Potencia limitada a 250 mW, antena instalable por el usuario. La FCC también permite la banda de 5.72–5.850 GHz con PIRE máxima de 4W.
  La FCC tiene en estos momentos una limitación transitoria sobre la operación en las bandas de 5600-5650 MHz.
- U-NII Alta (U-NII-3): 5.725 a 5.825 GHz.

Para PtP en la banda de 5 GHz la máxima PIRE es mayor ya que una antena de ganancia alta produce un haz muy estrecho y por lo tanto la interferencia causada a otros usuarios es mucho menor que en la topología PtMPt.

Certificación de equipos

Los gobiernos en muchos países piden una certificación formal de que un equipo de radio específico cumpla con estándares técnicos determinados y con regulaciones locales. A esto se le llama *homologación* y el proceso debe hacerlo un laboratorio independiente autorizado por el gobierno del país respectivo.

Los equipos certificados pueden operar sin licencia individual. Cabe hacer notar que la certificación es sólo válida para el estado original de fábrica de los equipos de radio. Por ejemplo, cambiar la antena en un punto de acceso en los EEUU invalida la certificación de la FCC.

Normas de Uso del ISP

Muchos ISP (Internet Service Provider) incluyen en sus “Normas de Uso” una cláusula que prohibe a los usuarios compartir la conexión a Internet. Puede también haber conexiones comerciales que no tengan estas limitaciones. Es importante notar que esto NO es materia legal sino una cláusula del contrato con el ISP, y que la repercusión de contravenir dicha cláusula es normalmente la desconexión del servicio de Internet.

4. ESPECTRO RADIOELÉCTRICO

¿Qué es el espectro radioeléctrico?

No existe una definición simple de espectro radioeléctrico. Desde el punto de vista técnico, el espectro es el rango de ondas electromagnéticas que pueden utilizarse para transmitir información. Desde el punto de vista práctico, los aspectos económicos y políticos, así como la tecnología usada para transmitir la información por medio de esas ondas juegan un papel crucial. Para dar un ejemplo, cuando Marconi en 1902 atravesó el Atlántico por primera vez con su "mensaje telegráfico inalámbrico", utilizó la totalidad del espectro disponible en su época para enviar unos pocos bits/s por un área de miles de kilómetros cuadrados. Con el transmisor de chispa usado para este logro que ocupó todas las frecuencias que los receptores existentes podían captar, nadie más podía usar la radio para comunicarse en un radio de unos 3500 km desde la estación transmisora en Inglaterra.
Si otros usuarios querían enviar mensajes en la misma área, hubieran necesitado coordinar sus transmisiones en diferentes "franjas de tiempo" para poder compartir el medio. Esta técnica se llama Acceso Múltiple por División de Tiempo o **TDMA** por su sigla en inglés (*Time Division Multiple Access).* Los usuarios situados a distancias mucho mayores de 3500 km desde el transmisor de Marconi, podían usar el espectro de nuevo ya que la potencia de las ondas de radio disminuye a medida que se alejan del transmisor. La reutilización del espectro en diferentes áreas geográficas se denomina Acceso Múltiple por División de Espacio o SDMA por su sigla en inglés (Space Division Multiple Access). Posteriormente, Marconi construyó un transmisor capaz de restringir las emisiones a sólo un rango de frecuencias y un receptor que podía "sintonizarse" para un rango particular de frecuencias. Ahora, múltiples usuarios podían transmitir simultáneamente en la misma área (espacio) y al mismo tiempo. Había nacido la FDMA, (Frequency Division Multiple Access) el Acceso Múltiple por División de Frecuencias. Así la radio se convirtió en un medio práctico de comunicación y el único que podía alcanzar un barco en mar abierto.
La coordinación de las frecuencias asignadas a los diferentes usuarios la efectuaron las agencias nacionales creadas para este efecto, pero como las ondas de radio no se detienen en las fronteras nacionales, se necesitaron acuerdos internacionales.

La organización internacional que regulaba la transmisión de telegramas entre los diferentes países fue comisionada para asignar el uso del espectro electromagnético.

Hoy en día, la Unión Internacional de Telecomunicaciones, ITU, es la organización internacional más antigua que tiene la tarea de emitir recomendaciones para las 139 naciones que la integran sobre cuáles frecuencias se deben utilizar para cada servicio.

El uso del espectro para aplicaciones militares planteó un nuevo problema: el de "*jamming*", como se definió la interferencia intencional introducida por el enemigo para impedir la comunicación. Para evitar el *jamming,* se inventó una nueva técnica por la cual la información transmitida se combinaba con una especie de código matemático especial con lo cual solamente los receptores con el conocimiento de ese código podían interpretar la información. La señal codificada se transmitía a baja potencia, pero usando un intervalo muy amplio de frecuencias para hacer el *jamming* más difícil.

Esta técnica se adoptó más tarde para aplicaciones civiles en lo que se llama Acceso Múltiple por División de Código, o CDMA (Code Division Multiple Access), uno de los aditamentos de la comunicación de espectro extendido (spread spectrum communication), usado ampliamente en los sistemas modernos de comunicación. Resumiendo, el espectro puede ser utilizado por múltiples usuarios por medio de la asignación de diferentes franjas de tiempo, diferentes intervalos de frecuencia, diferentes regiones del espacio, o diferentes códigos. Una combinación de todos estos métodos se encuentra en los últimos sistemas celulares. Además de los asuntos de la soberanía y su defensa, hay fuertes intereses económicos y políticos que juegan un papel determinante en el manejo del espectro, el cual, a su vez, debe ser constantemente actualizado para aprovechar los avances de las tecnologías de la comunicación.

Gracias al avance constante de las técnicas de modulación y codificación, la ingeniería de telecomunicaciones descubre formas cada vez más eficientes de transmitir información utilizando diversidad de tiempo, frecuencia y espacio. Su objetivo es aumentar la "eficiencia del espectro", que se define como la cantidad de bits por segundo (bits/s) que puede transmitirse en cada Herzio (Hz) del espectro por kilómetro cuadrado de área. Por ejemplo, los primeros intentos de prestación de servicios de telefonía móvil empleaban un transmisor potente situado en un lugar conveniente para dar cobertura a toda una ciudad. Este transmisor (llamado **Estación Base**, en este contexto) dividía la banda de frecuencias

asignada en cierta cantidad de canales, digamos 30, de tal manera que se podían mantener sólo 30 conversaciones de forma simultánea en toda la ciudad. En consecuencia, el servicio era muy caro y sólo las personas muy ricas podían darse ese lujo. Esta situación se mantuvo durante muchos años hasta que los avances en la tecnología electrónica permitieron la implementación de un plan para aprovechar la "diversidad del espacio". En lugar de utilizar un transmisor único de gran alcance para cubrir toda la ciudad, el área de servicio se dividió en muchas "células", cada una provista de un transmisor de baja potencia. Las células que están suficientemente separadas pueden utilizar los mismos canales sin interferencias. Esto se conoce como reutilización de frecuencias.
Con la estrategia celular, los primeros 10 canales usan la banda de frecuencia 1; los segundos 10 canales la banda de frecuencia 2; y los restantes 10 canales la banda de frecuencia 3. Esto se muestra en la Figura 1 donde los colores corresponden a las diferentes bandas de frecuencia. Nótese que los colores se repiten sólo a distancias suficientes como para evitar interferencia. Si dividimos la ciudad en 50 células, por ejemplo, podemos tener 10 x 50 = 500 usuarios/as simultáneos/as en la misma ciudad en lugar de 30. Por lo tanto, al agregar células más pequeñas (con una potencia de transmisión más baja) podemos aumentar el número de canales disponibles hasta llegar al límite que impone la interferencia.

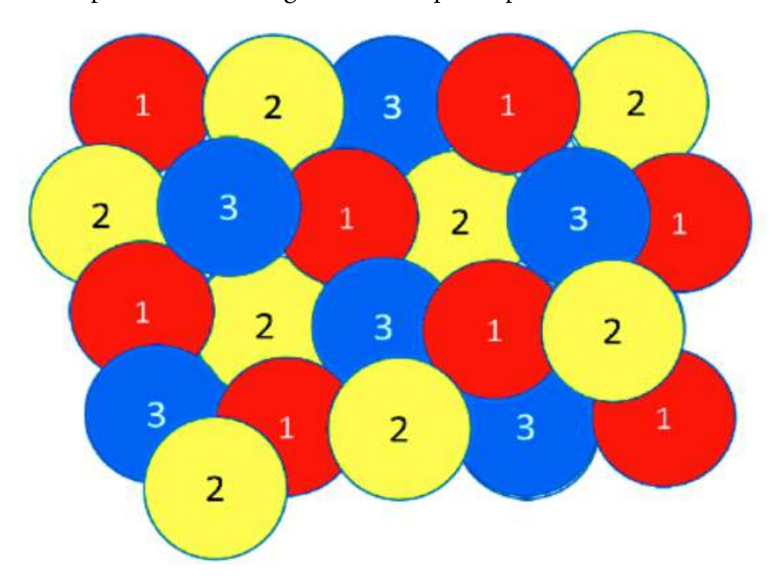


Figura ER 1: Compartición celular del espectro

Este ejemplo muestra que el uso inteligente de los recursos existentes puede aumentar drásticamente la eficiencia.
Aunque el uso principal del espectro es para efectos de comunicación, existen también otros usos como la cocción de alimentos en hornos de microondas, ciertas aplicaciones médicas, los comandos remotos de puertas de garaje, etc.
Algunas bandas de frecuencia se asignan para estos fines en lo que se conoce como las bandas industriales, científicas y médicas (bandas ICM o ISM en inglés). Este empleo del espectro suele ser para aplicaciones de corta distancia.

En 1985 se produjo un gran avance cuando la Comisión Federal de Comunicaciones (FCC en inglés), el organismo que supervisa el espectro en Estados Unidos, permitió el uso de este espectro para aplicaciones de comunicaciones, siempre que la potencia de transmisión se mantuviera en un nivel muy bajo para minimizar las interferencias.
Las personas pudieron entonces usar libremente estas bandas “sin licencia” sin necesidad de solicitar un permiso, siempre que los equipos empleados estuvieran certificados por un laboratorio autorizado que garantizara el cumplimiento de las medidas de atenuación de interferencia.

Varios fabricantes aprovecharon esta oportunidad para ofrecer equipos de computación que podían comunicarse entre sí sin necesidad de cables, y se construyeron redes inalámbricas para transmisión de datos que cubrían importantes áreas geográficas.
Sin embargo, el punto de inflexión llegó en 1997 cuando el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, en inglés aprobó el estándar 802.11, la base de lo que se conoce ahora como WiFi.

La existencia de un estándar que garantizaba la interoperabilidad de los equipos producidos por diferentes fabricantes estimuló un impresionante crecimiento del mercado, lo que a su vez impulsó la competencia que condujo a un descenso drástico del costo de los equipos.
En particular, la porción de la banda ICM (ISM) entre 2400 y 2483 MHz hoy en día está disponible en la mayor parte del mundo sin necesidad de licencia y la utilizan ampliamente las portátiles, las tabletas, los teléfonos inteligentes e incluso las cámaras fotográficas.

Es importante subrayar el rol que ha tenido el espectro sin licencia en el acceso WiFi a Internet de alta velocidad. Muchos aeropuertos, hoteles y cafés de todo el mundo ofrecen acceso WiFi gratuito en sus espacios, y se han construido redes comunitarias inalámbricas de bajo costo que cubren importantes áreas geográficas tanto en zonas rurales como urbanas, todo gracias a la disponibilidad del espectro sin licencia.
Los operadores de telefonía móvil que tienen que pagar bastante por las licencias para el uso del espectro se mostraron hostiles ante esta aparente competencia desleal. Sin embargo, cuando ellos comenzaron a vender teléfonos inteligentes, que hacen un gran uso de Internet, se dieron cuenta de que podían descargar el tráfico hacia WiFi en beneficio propio, ya que esto aliviaba el tráfico en su red de distribución, lo que se conoce como backhaul.
Actualmente, estos operadores alientan a sus clientes al uso de WiFi donde esté disponible y a utilizar el servicio, más caro, de telefonía celular sólo cuando estén fuera del alcance de algún punto de acceso WiFi.
Esto es un ejemplo notable del valor del espectro sin licencia incluso para los operadores de telecomunicaciones tradicionales, que a menudo han presionado en su contra.

¿Cómo se adjudica el espectro?

Hoy en día, los métodos principales para acceder a una banda determinada del espectro son las licitaciones y los llamados “concursos de belleza”.

El método de licitación es muy directo: las partes interesadas pujan por una porción determinada de la banda de frecuencia y quien haga la oferta más alta, obtiene el derecho a usarla.
En teoría este método garantiza la transparencia en la adjudicación.
En la práctica, este método ha sido vulnerado, y ha habido casos de poderosos intereses comerciales que han adquirido bandas de frecuencia sólo para evitar su uso por la competencia, lo que resulta en la inutilización de una porción valiosa del espectro.
También existe la tentación por parte de los gobiernos de utilizar este método como un medio de generación de ingresos y no precisamente en pro del interés público.
Como ejemplo, en el 2000 hubo subastas en varios países europeos para asignar espectro para teléfonos móviles que produjeron una ganancia de 100.000 millones de euros para las arcas de los gobiernos.

El método del "concurso de belleza" requiere que las partes interesadas presenten propuestas sobre la forma en que van a utilizar el espectro. Luego, un comité del ente regulador del espectro decide cuál de las propuestas sirve mejor a los objetivos públicos. Este método se basa en la objetividad, competencia técnica y honestidad de los miembros del comité, lo que no siempre puede garantizarse.

En muchos países hay normas para la adjudicación del espectro que exigen la renuncia a las bandas del espectro adquiridas anteriormente que no se utilizan. Sin embargo, estas normas a menudo no se aplican debido a los fuertes intereses económicos en juego.



Figura ER 2: Vehículo especial para supervisión del espectro en Montevideo, Uruguay.

La Figura ER 2 muestra una fotografía de un vehículo que monitorea el espectro en Montevideo, Uruguay.

En la figura ER 3 vemos el mismo tipo de equipo utilizado en Jakarta, Indonesia.

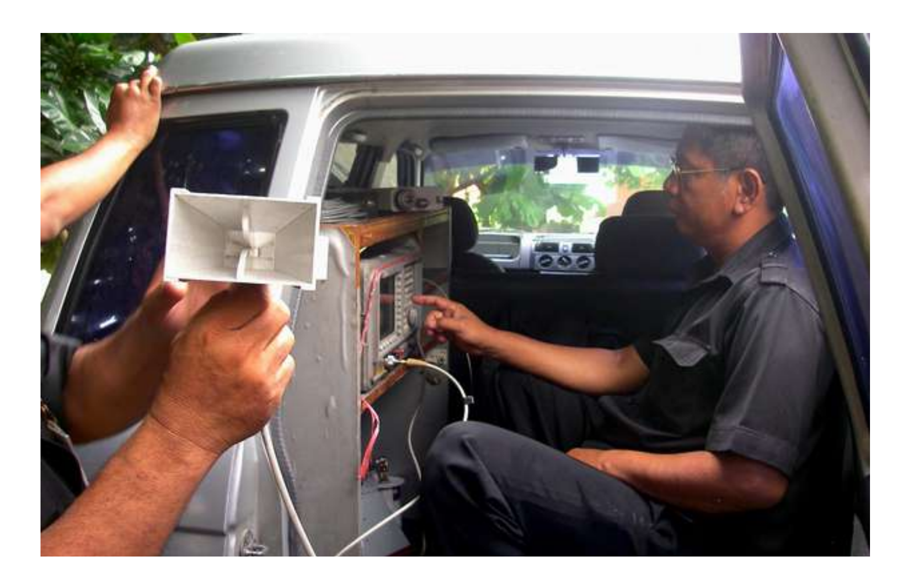


Figura ER 3: La "Policía del espectro" en acción en Jakarta, Indonesia

Hay que hacer notar que el espectro abierto que se usa en bandas sin licencia no puede evitar los problemas de interferencia, especialmente en zonas densamente pobladas. Sin embargo, el espectro abierto ha demostrado ser un éxito para aplicaciones de corta distancia en las ciudades y de larga distancia en zonas rurales. Por lo tanto, es aconsejable investigar nuevas formas de asignación del espectro teniendo en cuenta las necesidades de las diversas partes interesadas y estableciendo un equilibrio entre ellas. Los avances de la tecnología más recientes hacen que un mecanismo dinámico de asignación del espectro sea la mejor opción.

Como comparación, el método actual de asignar de espectro es semejante al sistema de ferrocarriles donde las vías del tren pueden estar inactivas por un tiempo considerable, mientras que la asignación dinámica del espectro es similar al sistema de autopistas que puede ser usada en todo momento por los diferentes usuarios.

Aspectos políticos

No puede desestimarse la importancia del espectro como facilitador de las comunicaciones. La televisión y la radio tienen una fuerte influencia en la formación de las percepciones del público sobre cualquier tema y se han utilizado abiertamente para propaganda política.

Se ha dicho, por ejemplo, que la elección de Kennedy como presidente de Estados Unidos se debió principalmente a su campaña por televisión. Durante la guerra fría, *La Voz de América, Radio Moscú* y *Radio Habana Cuba* eran medios muy efectivos para influir en el público mundial.
Ejemplos más recientes incluyen la influencia de CNN y Al Jazeera en dar forma a la interpretación pública de la Primavera Árabe. El espectro que se utiliza para la comunicación de dos vías, incluidas las tecnologías móviles y de internet, también ha sido objeto de intervenciones de los gobiernos, especialmente en casos de inestabilidad política. Por otra parte, los intereses económicos también desempeñan un papel vital en la radiodifusión; la sociedad de consumo depende mucho de la radio y la televisión para crear necesidades artificiales o para inclinar al consumidor hacia una marca particular. Podemos concluir diciendo que el espectro electromagnético es un recurso natural cuya utilidad está fuertemente condicionada por factores tecnológicos, económicos y políticos.

Explosión de la demanda de espectro

A medida que el número de tabletas y teléfonos inteligentes crece, los operadores de telecomunicaciones compiten por el acceso a nuevas bandas de frecuencia. Sin embargo, los métodos tradicionales de adjudicación del espectro se enfrentan a un callejón sin salida.

Debemos tener en cuenta que el espectro se utiliza para emisiones de radio y televisión, comunicaciones satelitales, control del tráfico aéreo, geolocalización (Sistemas de Posicionamiento Global: **GPS** por su sigla en inglés); también para objetivos militares, policiales y otros propósitos gubernamentales. En general, la demanda de espectro adicional se cubre gracias a los avances en electrónica que permiten el uso de frecuencias más altas a costos asequibles. Estas frecuencias son muy adecuadas para las transmisiones de alta velocidad, pero tienen un alcance limitado y las paredes y otros obstáculos, así como la lluvia, las atenúan en exceso.

Por ejemplo, comparemos la cobertura de una estación de radio AM con la de una emisora de FM: el gran alcance de la radio AM se debe a que emplea frecuencias más bajas. Por el contrario, las estaciones de FM usan anchos de banda mayores por lo que pueden ofrecer una mayor calidad de audio pero a expensas de un alcance más limitado.

En consecuencia, las frecuencias de difusión televisiva son codiciadas por los proveedores de telefonía celular: el uso de frecuencias más bajas significa que se necesitan menos estaciones base, con el correspondiente ahorro en despliegue, operación y mantenimiento. Debido a ello, a estas frecuencias se las llama comúnmente la flor y nata del espectro.

El mayor impacto de los métodos de codificación y modulación avanzados para un uso más eficiente del espectro ha sido la disponibilidad de más bits/s por Hz de ancho de banda. Esto es económicamente posible gracias a los grandes avances en electrónica (como la fabricación de circuitos integrados más avanzados) que ahora hacen asequible la implementación de las técnicas sofisticadas de modulación y codificación necesarias.

Según los cálculos realizados en 1948 por Claude Shannon, el padre de las telecomunicaciones modernas, una línea telefónica normal podría, en teoría, transportar hasta 30 kbit/s. Pero esa tasa sólo se logró en la década de 1990 con la invención de circuitos integrados que podían implementar las técnicas requeridas. En particular, la transición a la transmisión de televisión digital terrestre, que es más eficiente en el uso del espectro en comparación con la transmisión analógica, ha liberado parte del espectro en los "Espacios Blancos de televisión", o TVWS (*TV White Spaces* en inglés). Los TVWS son las frecuencias entre los canales de televisión analógica que hubo que dejar sin utilizar para evitar interferencias.

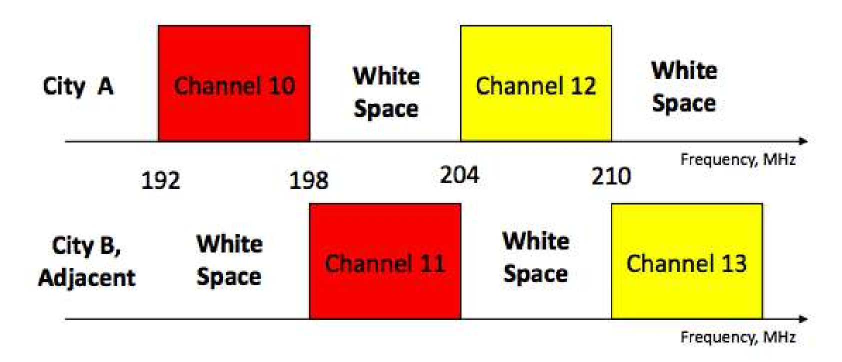


Figura ER 4: Ejemplo de adjudicación de canales de TV en dos ciudades que están tan cerca que las transmisiones de una alcanzan a la otra. Los espacios blancos se mantienen inutilizados para reducir la interferencia

En la transmisión tradicional de televisión analógica, los canales adyacentes no se pueden utilizar al mismo tiempo, porque la señal de un canal se "derramaría" hacia los dos canales adyacentes causando interferencia.
Esto es similar a la medianera que separa los dos sentidos del tráfico de las autopistas para evitar colisiones. Se debe dejar un "Espacio Blanco" entre dos canales contiguos de televisión analógica para evitar interferencia.
La emisión de televisión digital usa el espectro de forma mucho más eficiente: se pueden acomodar varios canales en la misma banda de frecuencia que antes usaba un único canal analógico, sin "derrame" hacia los canales adyacentes. Allí donde se sustituye la televisión analógica por la digital es posible cosechar un "dividendo digital".

En conclusión, el concepto de Espacio Blanco puede aplicarse a tres grupos de frecuencias:

- Al espectro asignado a la emisión de televisión pero que actualmente no se utiliza. Esto se aplica en particular a los países en desarrollo, en donde no ha habido ningún incentivo económico para que las emisoras usen todos los canales de TV disponibles.
- Al espectro que se debe dejar libre entre dos canales de televisión adyacentes para evitar interferencias.
- Al espectro recuperado al hacerse efectiva la transición a la televisión digital terrestre. Esto se aplica actualmente a los países desarrollados, pero pronto se aplicará también a los países en desarrollo.

En los últimos 20 años se experimentó un crecimiento tremendo de la demanda de espectro para servicios de comunicaciones móviles. Al respecto, los servicios de datos están consumiendo mucho más ancho de banda que la voz y el creciente uso del video presenta un desafío adicional. No es sorprendente que los operadores de telecomunicaciones en todas partes compitan por una porción de estos "Espacios Blancos". Asimismo, las emisoras son muy reacias a ceder espectro a sus competidores directos.

¿Escasez o acaparamiento del espectro?

A pesar de que actualmente en los países desarrollados todo el espectro disponible está asignado, varios estudios independientes han demostrado que la cantidad total de espectro en uso en cualquier momento y en cualquier lugar es apenas una pequeña fracción del total. Esto se debe a la forma en que el espectro fue asignado originalmente y al hecho de que el espectro se utiliza a menudo de forma intermitente; por ejemplo algunas emisoras de TV no transmiten las 24 horas del día.

Como consecuencia, se sugirió una forma radicalmente nueva para el uso del espectro. En vez de otorgar la concesión del espectro a una organización determinada de forma exclusiva, un nuevo paradigma dinámico de gestión del espectro propone usar cualquier espectro disponible en un lugar y en un momento determinado y cambiar a otra frecuencia cada vez que se detecta una interferencia en una determinada banda.

Se puede hacer una analogía para explicar este concepto: la forma actual de asignar el espectro es semejante al de una vía férrea donde las vías nunca se usan el 100% del tiempo. Se podría hacer un uso más eficiente de la misma extensión de terreno con una autopista donde muchos usuarios diferentes pueden compartir el mismo trayecto de acuerdo con sus necesidades particulares.

Naturalmente, la implementación del acceso dinámico al espectro requiere nuevas tecnologías y nueva legislación y hay muchos intereses creados que luchan contra esto, alegando posibles interferencias. La cuestión clave es cómo determinar cuándo una banda específica del espectro está realmente en uso en una región geográfica en particular y cómo cambiar rápidamente a una nueva banda de frecuencia cuando se detecta la existencia de un usuario con mayor prioridad. La tecnología para lograr esta proeza se demuestra e implementa en el nuevo estándar IEEE 802.22 de reciente aprobación, así como en otras normas actualmente en consideración.

IEEE 802.22

Estimulado por el éxito impresionante del WiFi (debido principalmente al uso del espectro sin licencia o abierto), el IEEE creó un grupo de trabajo para atender las necesidades de una Red Inalámbrica de Área Regional. El reto consistía en desarrollar una tecnología adecuada para transmisión de larga distancia que pudiera implementarse en distintos países (cada uno con asignaciones de espectro muy diferentes). El IEEE se centró en el espectro asignado actualmente a la emisión de TV que se extiende desde 50 a 800

MHz aproximadamente. Este rango del espectro no se utiliza en su totalidad todo el tiempo, por lo que quedan “Espacios Blancos”, es decir, regiones en desuso que pueden ser re-usadas para comunicaciones bidireccionales. En las zonas rurales de todo el mundo, pero especialmente en los países en desarrollo, existen grandes porciones de espectro subutilizadas. Es probable que el estándar IEEE 802.22 habilite el acceso al espectro dinámico de una manera similar a como lo hizo el estándar IEEE 802.11 (WiFi) para el espectro abierto. Por supuesto que no todo el espectro puede ser liberado a la vez; se necesita un proceso gradual en tanto se resuelven los muchos obstáculos técnicos, legales, económicos y políticos. No hay duda, sin embargo, de que el IEEE 802.22 abre el camino para el futuro de la asignación del espectro. Para evaluar la disponibilidad de un determinado canal de frecuencia en un momento dado, se consideran dos métodos: detección de canal y una base de datos de usuarios primarios en un determinado lugar geográfico en un momento dado. La detección de canal significa que antes de usar un canal, las estaciones base tendrán que escucharlo primero para determinar si ya está en uso. Si lo está, la estación base intentará con otro canal y repetirá el procedimiento hasta encontrar un canal libre. El dispositivo continuará detectando a intervalos regulares en la eventualidad de que otras estaciones comiencen a emitir en cualquier momento. Aunque este método debería ser suficiente para detectar y evitar la interferencia del espectro, los titulares actuales de espectro han presionado con éxito a los entes reguladores para obligar a la implementación del segundo método, que es mucho más complicado e impone al usuario costos adicionales en equipos. El segundo método establece una zona “restringida” en un canal dado mediante la construcción de una base de datos de las estaciones de transmisión existentes, incluyendo su posición y área de cobertura respectiva.

Una nueva estación que desee transmitir debe primero determinar su posición exacta (por lo que debe tener un receptor GPS u otros medios para averiguar su ubicación geográfica) y luego consultar a la base de datos para comprobar que su ubicación actual no se encuentre en la zona prohibida del canal que está tratando de utilizar. Para realizar la consulta debe tener acceso a Internet por algún otro medio (ADSL: *Asymmetrical Digital Subscriber Loop*, cable, satélite o celular), aparte de la radio 802.22 (que no se puede utilizar hasta tener confirmación de que el canal esté disponible).
Esto agrega una carga extra para el hardware de la estación y se traduce en un costo adicional aparte del costo de construir y mantener la base de datos.

En Estados Unidos, la FCC (*Federal Communications Commission*: la agencia reguladora del espectro) promueve la elaboración de una base de datos de usuarios registrados del espectro TVWS y autorizó a 10 empresas privadas diferentes a construir, operar y mantener dicha base. Además, están realizando instalaciones piloto con el estándar (IEEE 802.22). En el Reino Unido, OFCOM, (el ente regulador del espectro) también está llevando a cabo ensayos con el IEEE 802.22. OFCOM usa el método de base de datos y ha descartado el método de detección de ocupación del canal como manera de evitar la interferencia. Aunque el estándar IEEE 802.22 ha recibido la mayor publicidad, actualmente están en estudio varias normas que compiten por los Espacios Blancos de televisión para los servicios de comunicación bidireccional. Estas son:

IEEE 802.11af

Esta enmienda se basa en el enorme éxito de IEEE 802.11 y adapta la misma tecnología para las bandas de frecuencias asignadas a la transmisión de televisión. Esta adaptación alivia el hacinamiento del espectro en la banda de 2.4 GHz y ofrece un mayor alcance gracias al uso de frecuencias de transmisión más bajas. Un grupo de trabajo de IEEE 802.11 está discutiendo los detalles.

IEEE 802.16h

Esta enmienda del estándar 802.16 fue ratificada en 2010 y describe el mecanismo para implementar el protocolo en operaciones descoordinadas y aplicaciones con o sin licencia. Aunque la mayoría de las implantaciones se ha dado en la banda de 5 GHz, también se puede aplicar a las bandas de frecuencias de televisión y puede beneficiarse de la importante implantación de los sistemas WiMAX (Acceso Inalámbrico por Microondas: *Wireless Microwave Access*) en muchos países.

Ventajas de los países en desarrollo

En los países en desarrollo, el espectro asignado a la televisión se utiliza sólo parcialmente. Esto representa una magnífica oportunidad para introducir servicios inalámbricos de redes de datos en los canales que no están actualmente en uso, y para comenzar a recoger los beneficios de TVWS en un entorno más favorable, donde puede no ser necesario el tipo de detección de espectro y la agilidad para realizar cambios frecuentes que se necesitan para compartir el espectro superpoblado de los países ricos.

La implantación exitosa de los sistemas de telefonía móvil CDMA en la banda de 450 MHz (en el centro de las frecuencias asignadas a televisión) ha demostrado el valor de las frecuencias más bajas para las comunicaciones bidireccionales de datos, por ejemplo, en una zona rural de la región argentina de la Patagonia, que actualmente atiende la Cooperativa Telefónica de Calafate (COTECAL). COTECAL ofrece servicios de voz y datos a clientes que se encuentran a distancias de hasta 50 km de la estación base, en la hermosa región que se muestra en la siguiente figura.



Figura ER 5: Región asistida con servicios de datos y voz por COTECAL, en Calafate y El Chaltén, Argentina

Mientras se discuten los diversos aspectos de la transición digital, se abre una oportunidad para que las personas interesadas incidan a favor de la introducción de soluciones basadas en TVWS, para asegurar que los intereses comerciales no prevalezcan sobre los intereses de la sociedad en general. Los/as activistas deben hacer hincapié en la necesidad de transparencia en el proceso de asignación de frecuencias.
En particular, deben exigir la rendición de cuentas de la gestión gubernamental y de los titulares de espectro actuales, de tal manera que el uso del espectro en cada región del propio país sea transparente.

El monitoreo del espectro requiere de instrumentos costosos y complicados para aprender a usarlos. Sin embargo, existe un dispositivo de reciente aparición, asequible y fácil de usar, que analiza la banda de frecuencias entre 240 y 960 MHz, que abarca la porción superior de la banda de TV.
Más detalles sobre este hardware de código abierto llamado Analizador de Espectro de Radiofrecuencia Explorer para la banda superior de TV se encuentran en: www.seeedstudio.com/depot/rf-explorer-model-wsub1g-p-922.html
La figura ER 6 muestra el explorador de radiofrecuencia para la banda de 2.4 GHz probando una antena construida por los participantes del taller de capacitación en tecnologías inalámbricas del Centro Internacional de Física Teórica (ICTP en inglés) en febrero de 2012 en Trieste, Italia.



Figura ER 6: Participantes de Albania, Nepal, Malawi e Italia probando una antena con el Analizador de Espectro RF Explorer en Trieste, febrero de 2012

Este instrumento de bajo costo allana el camino para una amplia participación de la gente en la medición de la utilización real del espectro en cada país, lo que esperamos conduzca a una mejor gestión del espectro.

Información adicional en:
http://www.apc.org/en/faq/citizens-guide-airwaves

5. ANTENAS / LÍNEAS DE TRANSMISIÓN

El transmisor que genera la energía de RF (radiofrecuencia) para entregar a la antena generalmente está ubicado a cierta distancia de los terminales de la misma. El enlace entre ambos es la ***línea de transmisión de RF***. Su propósito es transportar la energía de RF desde un lugar hacia el otro de la forma más eficiente posible. Del lado del receptor, la antena es responsable de captar las señales de radio desde el aire y pasarlas al receptor con la mínima cantidad de distorsión, para que el radio pueda descodificar la señal. Por estas razones el cable de RF tiene un rol muy importante en los sistemas de radio: debe mantener la integridad de las señales en ambas direcciones.

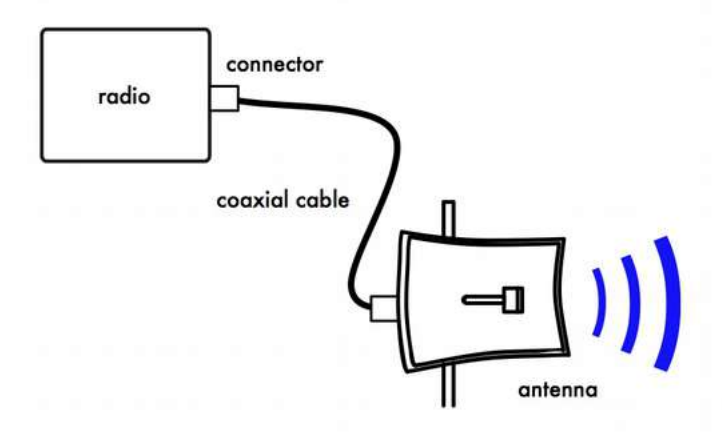


Figura ALT 1: Radio, línea de transmisión y antena

La línea de transmisión más simple que podamos imaginar es la bifilar o de dos hilos, que consiste en dos conductores separados por un dieléctrico o aislante. El dieléctrico puede ser aire o un plástico como el que se usa para líneas de transmisión planas en antenas de TV.

Una línea de transmisión bifilar abierta en un extremo no va a irradiar porque la corriente en cada cable tiene el mismo valor pero una dirección opuesta, de manera que los campos creados en un punto dado a alguna distancia de la línea se cancelan.

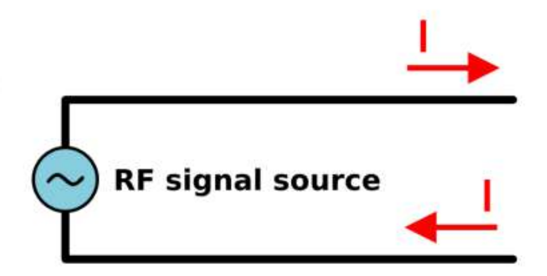


Figura ALT 2: Línea de transmisión bifilar

Si doblamos los extremos abiertos de la línea de transmisión en sentidos opuestos, la corriente va a generar campos eléctricos que están en fase y se refuerzan mutuamente, y, por lo tanto, irradiarán y se propagarán a distancia. Ahora tenemos una antena en un extremo de la línea de transmisión.

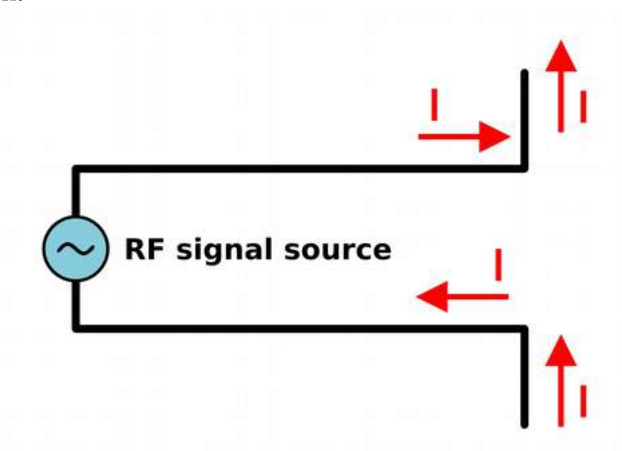


Figura ALT 3: Línea de transmisión convertida en antena

El largo de la porción doblada de la línea de transmisión va a determinar la característica de la antena. Si el largo corresponde a un cuarto de la longitud de onda, vamos a tener una antena dipolo de media onda con una ganancia de 2,15 dBi.La presencia de metales en las cercanías va a afectar profundamente el funcionamiento de la línea de transmisión bifilar descrita, así que la mejor solución es confinar los campos eléctricos por medio de un conductor externo que proteja el interno.

Esto constituye un cable coaxial. Alternativamente, un tubo metálico hueco de dimensiones apropiadas también va a transportar eficazmente energía RF en lo que se llama *guía de onda*.

Cables

En el caso de frecuencias mayores que HF (alta frecuencia, por su sigla en inglés *High Frequency*) los cables utilizados son casi exclusivamente los coaxiales (o para abreviar ***coax***, derivado de las palabras del inglés "*of common axis*": eje en común). Los cables coaxiales tienen un conductor central recubierto por un material no conductor denominado ***dieléctrico***, o simplemente ***aislante***. El dieléctrico se recubre con una pantalla conductora envolvente a menudo en forma de malla. El dieléctrico evita una conexión eléctrica entre el conductor central y la pantalla. Finalmente, el coaxial está protegido por un recubrimiento generalmente de PVC. El conductor interior transporta la señal de RF, y la pantalla evita que la señal de RF sea radiada a la atmósfera, así como impide que posibles señales externas interfieran con la que está siendo transmitida por el cable. Otro hecho interesante es que las señales eléctricas de alta frecuencia siempre viajan a lo largo de la capa exterior del conductor central: cuanto más grande el conductor central, mejor va a ser el flujo de la señal. Esto se denomina "efecto pelicular".

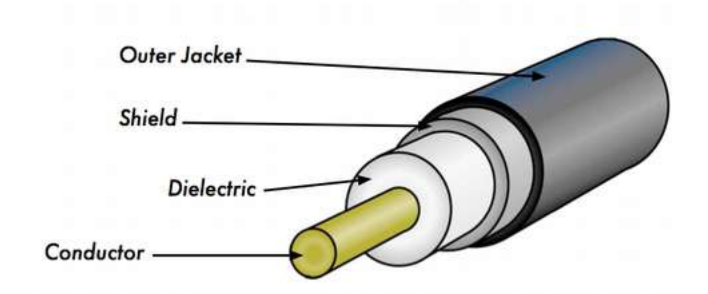


Figura ALT 4: Cable coaxial con recubrimiento (outer jacket), pantalla (shield), dieléctrico, y conductor central

A pesar de que la construcción del cable coaxial es muy buena para contener la señal en el cable, presenta algo de resistencia al flujo eléctrico: a medida que la señal viaja a través del cable disminuye su intensidad.

Este debilitamiento es conocido como atenuación, y para las líneas de transmisión se mide en decibeles por metro (dB/m). El coeficiente de atenuación es una función de la frecuencia de la señal y la construcción física del cable. Si se incrementa la frecuencia de la señal, también lo hace su atenuación. Obviamente se necesita minimizar la atenuación del cable cuanto más nos sea posible, esto puede hacerse mediante la utilización de cables muy cortos y/o de buena calidad.
Aquí les presentamos algunos puntos que se deben considerar cuando elegimos un cable para utilizarlo con dispositivos de microondas:

1. Cuanto más corto mejor La primer regla cuando instalamos un cable es la de hacerlo lo más corto posible. La pérdida de energía no es lineal, por lo tanto duplicar el largo del cable implica perder mucho más que el doble de energía. En el mismo sentido, si reducimos el largo del cable a la mitad vamos a tener mucho más que el doble de potencia en la antena. La mejor solución es poner el transmisor lo más cerca que podamos de la antena, incluso si esto implica colocarlo en una torre.
2. Cuanto más barato peor La segunda regla de oro es que todo el dinero que se invierta en comprar un cable de buena calidad es un buen negocio. Los cables baratos están pensados para ser utilizados con bajas frecuencias como VHF. Las microondas requieren de los cables de mejor calidad que haya disponibles.
3. Evite usar RG-58: fue pensado para redes Ethernet delgadas, CB o radio de VHF, no para microondas.
4. Evite usar RG-213 o RG-8: fueron diseñados para CB y radio de HF. En este caso, incluso si el diámetro es grande, la atenuación es significativa debido al aislante barato empleado.
5. Cuando sea posible, use el mejor cable LMR o su equivalente. LMX es una marca de cable coaxial disponible en varios diámetros que trabaja bien en las frecuencias de microondas. Los más usados son LMR-400 y LMR-600. Los cables Heliax son también muy buenos, pero caros y difíciles de usar.
6. Siempre que sea posible utilice cables que ya tengan los conectores, y que hayan sido probados en un laboratorio apropiado.
7. La instalación de los conectores en el cable es una tarea delicada y se hace difícil realizarla adecuadamente aún teniendo las herramientas necesarias.

8. Nunca pise los cables, no los doble demasiado o trate de desenchufar un conector halando el cable directamente. Este comportamiento puede cambiar las características mecánicas del cable y por ende su impedancia, provocar un cortocircuito entre el conductor interno y la pantalla o incluso dañar la línea.
9. Rastrear y reconocer este tipo de problemas no es tarea fácil, y esto puede llevar a un comportamiento impredecible del radioenlace.
10. Para distancias muy cortas, un cable delgado de buena calidad puede ser adecuado ya que no introduce demasiada atenuación.

Guías de ondaW

Arriba de los 2 GHz, la longitud de onda es lo suficientemente corta como para permitir una transferencia de energía práctica y eficiente por diferentes medios. Una guía de onda es un tubo conductor a través del cual se transmite la energía en la forma de ondas electromagnéticas. El tubo actúa como un contenedor que confina las ondas en un espacio cerrado. El efecto de Faraday atrapa cualquier campo electromagnético fuera de la guía. Los campos electromagnéticos son propagados a través de la guía de onda por medio de reflexiones en sus paredes internas, que son consideradas perfectamente conductoras. La intensidad de los campos es máxima en el centro a lo largo de la dimensión X, y debe disminuir a cero al llegar a las paredes, porque la existencia de cualquier campo paralelo a las mismas en su superficie causaría una corriente infinita en un conductor perfecto.
En la siguiente figura pueden verse las dimensiones X, Y, y Z de una guía de ondas rectangular:

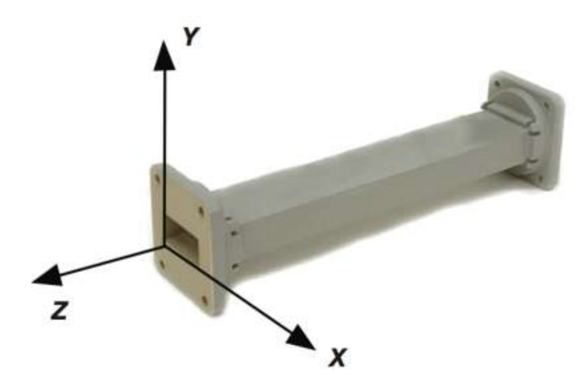


Figura ALT 5: Las dimensiones X, Y, y Z de una guía de onda rectangular

Hay un infinito número de formas en las cuales los campos eléctricos y magnéticos pueden organizarse en una guía de onda a frecuencias por encima de la frecuencia de corte. Cada una de esas configuraciones del campo se denomina modo. Los modos pueden separarse en dos grupos generales. Uno de ellos es el Transversal Magnético (TM por su sigla en inglés), donde el campo magnético es siempre transversal a la dirección de propagación, pero existe un componente del campo eléctrico en la dirección de propagación. El otro es el Transversal Eléctrico (TE por su sigla en inglés), en el que el campo eléctrico es siempre transversal, pero existe un componente del campo magnético en la dirección de propagación. El modo de propagación se identifica por dos letras seguidas por dos subíndices numéricos. Por ejemplo el TE 10, TM 11, etc. El número de modos posibles se incrementa con la frecuencia para un tamaño dado de guía, y existe un modo, llamado *modo dominante*, que es el único que se puede transmitir a la frecuencia más baja que soporta la guía de onda. En una guía rectangular, la dimensión crítica es X. Esta dimensión debe ser mayor que 0.5 λ a la frecuencia más baja que va a ser transmitida. En la práctica, generalmente la dimensión Y es igual a 0.5 X para evitar la posibilidad de que se opere en otro modo que no sea el modo dominante. Se pueden utilizar otras formas además de la rectangular, la más importante es la de tubo circular. Para éste se aplican las mismas consideraciones que para el rectangular. La dimensión de la longitud de onda para las guías rectangulares y circulares se presentan en la siguiente tabla, donde X es el ancho de la guía rectangular y r es el radio de la guía circular.

Todos los valores se refieren al modo dominante.

Tipo de guía	Rectangular	Circular
Longitud de onda de corte	2X	3.41r
Longitud de onda máxima transmitida con poca atenuación	1.6X	3.2r
Longitud de onda mínima antes de que se transmita el modo siguiente	1.1X	2.8r

La energía puede introducirse o extraerse de una guía de onda por medio de un campo eléctrico o magnético. Generalmente la transferencia de energía se da a través de una línea coaxial. Dos métodos posibles para acoplar una línea coaxial son utilizar el conductor interno de la línea, o a través de una espira.

Se puede introducir una sonda, constituida por una pequeña extensión del conductor interno de la línea coaxial, orientada paralelamente a las líneas de campo eléctrico. También se puede colocar un lazo o espira que encierre algunas de las líneas de campo magnético. El punto en el cual obtenemos el acoplamiento máximo depende del modo de propagación en la guía o en la cavidad. El acoplamiento es máximo cuando el dispositivo de acoplamiento está en el campo más intenso.

Si una guía de onda se deja abierta en uno de sus lados, puede radiar energía (es decir, puede ser usada como una antena en lugar de línea de transmisión). Esta radiación puede ser aumentada acampanando la guía de onda para formar una antena de bocina piramidal (horn).

Hay ejemplos de antenas hechas con guía de onda para para WiFi en el **Apéndice A** llamado Construcción de Antenas.

Conectores y adaptadores

Por medio de los conectores el cable puede ser conectado a otro cable o a un componente de la cadena de RF. Hay una gran cantidad de adaptadores y conectores diseñados para concordar con diferentes tamaños y tipos de líneas coaxiales. Describiremos algunos de los más populares.

Los conectores BNC fueron desarrollados a fines de los 40. La sigla BNC significa Bayoneta, Neill-Concelman, por los apellidos de quienes los inventaron: Paul Neill y Carl Concelman.

El tipo BNC es un conector miniatura de conexión y desconexión rápida. Tiene dos postes de bayoneta en el conector hembra, y el apareamiento se logra con sólo un cuarto de vuelta de la tuerca de acoplamiento. Los conectores BNC son ideales para la terminación de cables coaxiales miniatura o subminiatura (RG-58 a RG-179, RG-316, etc.). Tienen un desempeño aceptable hasta unos pocos cientos de MHz. Son los que se encuentran más comúnmente en los equipos de prueba y en los cables coaxiales Ethernet 10base2.

Los conectores TNC también fueron inventados por Neill y Concelman, y son una versión roscada de los BNC. Debido a que proveen una mejor interconexión por su conector de rosca, funcionan bien hasta unos 12 GHz. Su sigla TNC se debe al inglés (Neill-Concelman con Rosca, por *Threaded Neill-Concelman*).

Los conectores Tipo N (también por Neill, aunque algunas veces atribuidos a "Navy") fueron desarrollados originalmente durante la Segunda Guerra Mundial. Se pueden utilizar hasta a 18 GHz y se utilizan comúnmente en aplicaciones de microondas. Se fabrican para la mayoría de tipos de cable. Las uniones del cable al conector macho o hembra son supuestamente impermeables, lo que da un agarre efectivo. Sin embargo, para uso en exteriores deberían envolverse en cinta autoaglomerante para evitar que el agua penetre.

SMA es un acrónimo de Sub Miniatura versión A, y fue desarrollado en los 60. Los conectores SMA son unidades subminiatura de precisión que proveen excelentes prestaciones eléctricas hasta más de 18 GHz. Estos conectores de alto desempeño son de tamaño compacto y tienen una extraordinaria durabilidad.

Los SMB cuyo nombre deriva de Sub Miniatura B, son el segundo diseño subminiatura. Constituyen una versión más pequeña de los SMA con un acoplamiento a presión. Son adecuados hasta 4 GHz con un diseño de conector de presión.

Los conectores MCX se introdujeron en los 80.

Aunque utilizan contactos internos y aislantes idénticos a los SMB, el diámetro exterior de la clavija es 30% más pequeño que la del SMB. Esta serie proporciona opciones a los diseñadores cuando el peso y el espacio físico son limitados. MCX tiene una capacidad de banda ancha de 6 GHz con un diseño de conector a presión.

Además de estos conectores estándar, la mayoría de los dispositivos WiFi utilizan una variedad de conectores patentados. A menudo son simplemente conectores de microondas estándar con las partes centrales del conductor invertidas o con roscas a contramano.

Estos conectores especiales a menudo se acoplan a los otros elementos del sistema de microondas utilizando un cable delgado y corto llamado latiguillo, (en inglés ***pigtail***: cola de cerdo) que convierte el conector que no es estándar en uno más robusto y disponible comúnmente.

Entre estos conectores especiales tenemos:

RP-TNC. Es un conector TNC con el género invertido.

U.FL (también conocido como **MHF**). Probablemente es el conector de microondas más pequeño utilizado ampliamente en la actualidad. El U.FL /

MHF se utiliza para conectar una tarjeta de radio mini-PCI a una antena o a un conector más grande (como un N, o un TNC) usando un cable delgado en lo que se conoce como ***pigtail***.

La serie **MMCX**, también denominada MicroMate, es una de las líneas de conectores de RF más pequeñas desarrolladas en los 90. MMCX es una serie de conectores micro-miniatura con un mecanismo de bloqueo a presión que permite una rotación de 360 grados otorgándole gran flexibilidad.

Los conectores **MC-Card** son más pequeños y más frágiles que los MMCX. Tiene un conector externo con ranuras que se quiebra fácilmente luego de unas pocas interconexiones.

Los adaptadores coaxiales (o simplemente adaptadores), son conectores cortos usados para unir dos cables, o dos componentes que no se pueden conectar directamente. Los adaptadores pueden ser utilizados para interconectar dispositivos o cables de diferentes tipos. Por ejemplo, un adaptador puede ser utilizado para conectar un conector SMA a un BNC. También pueden servir para unir dos conectores del mismo tipo pero de género diferente.



Figura ALT 6: Adaptador N hembra de barrilito

Por ejemplo un adaptador muy útil es el que permite unir dos conectores machos Tipo N, que tiene dos conectores hembra en ambos extremos.

Elección del conector apropiado

“Una cuestión de género.” Casi todos los conectores tienen un género bien definido. Los conectores 'machos' tienen una carcasa externa o manga (frecuentemente con un hilo interno) que sirve para envolver el cuerpo del conector hembra. Normalmente tienen una clavija que se inserta en el enchufe correspondiente del conector hembra que tiene una carcasa roscada sobre la superficie o dos pines de bayoneta que sobresalen de un cilindro.

Tenga cuidado con los conectores de polaridad inversa, en los cuales el macho tiene un enchufe interno y el conector hembra una clavija interna.

Generalmente los cables tienen conectores macho en ambos extremos y los dispositivos de RF (por ej. transmisores y antenas) tienen conectores hembra. Los acopladores direccionales y dispositivos de medición de línea pueden tener tanto conectores macho como hembra. Los pararrayos, acopladores direccionales y dispositivos de medición line-through pueden tener tanto machos como hembras. Asegúrese de que cada conector macho en su sistema coincide con uno hembra.

“¡Menos es mejor!” Intente minimizar el número de conectores y adaptadores en la cadena de RF. Cada conector introduce alguna pérdida adicional, (!hasta unos pocos dB por cada conexión, dependiendo del conector!).

“!Compre, no lo haga usted mismo!” Como mencionamos anteriormente, siempre que pueda es mejor que compre cables que ya estén terminados con los conectores que usted necesite. Soldar los conectores no es una tarea sencilla, y en el caso de conectores pequeños como los U.FL y MMCX hacerlo bien es casi imposible. Hasta la conectorización de cables de foam (espuma) es ardua. No use BNC para frecuencias de 2.4 GHz o más altas. Utilice los conectores tipo N (o SMA, SMB, TNC, etc.).

Los conectores de microondas son componentes de precisión y se pueden dañar fácilmente si se manipulan mal. Como regla general, debe rotar la manga exterior para apretar el conector, dejando el resto del conector (y el cable) estacionario. Si se tuercen otras partes del conector mientras estamos ajustándolo, o aflojándolo, es muy posible que las mismas se rompan.

Nunca pise, ni deje caer los conectores en el piso cuando desconecte los cables (esto sucede más a menudo de lo que usted se imagina, especialmente cuando trabajamos en un mástil sobre un techo).

Nunca utilice herramientas como las pinzas para apretar los conectores. Hágalo siempre con sus manos. Cuando trabaje en exteriores recuerde que los metales se expanden a altas temperaturas y reducen su tamaño a baja temperatura: un conector muy apretado puede dilatarse en el verano o quebrarse en el invierno.

Antenas y patrones de radiación

Las antenas son un componente muy importante de los sistemas de comunicación. Por definición, una antena es un dispositivo utilizado para transformar una señal de RF que viaja en una línea de transmisión, en una onda electromagnética en el espacio abierto. Las antenas poseen una propiedad conocida como reciprocidad, lo cual significa que una antena va a mantener las mismas características sin importar si está transmitiendo o recibiendo. Todas las antenas operan eficientemente en una banda de frecuencia relativamente baja. Una antena debe ser sintonizada en la misma banda que el sistema de radio al que está conectada, de lo contrario, la recepción y transmisión se ven afectadas. En la radiodifusión podemos conformarnos con antenas receptoras ineficientes porque los transmisores son muy potentes, pero en una comunicación en ambos sentidos hay que tener antenas de tamaño apropiado. Cuando se alimenta la antena con una señal, emitirá radiación distribuida en el espacio de cierta forma. La representación gráfica de la distribución relativa de la potencia radiada en el espacio se llama diagrama o patrón de radiación.

Glosario sobre antenas

Antes de hablar de antenas específicas, hay algunos términos que deben ser definidos y explicados:

Impedancia de entrada

Para una transferencia de energía eficiente, la impedancia del radio, la antena, y el cable de transmisión que las conecta debe ser la misma.

Las antenas y sus líneas de transmisión generalmente están diseñadas para una impedancia de 50Ω. Si la antena tiene una impedancia diferente a 50Ω, hay una desadaptación y se va a producir reflexión a menos que se añada un circuito de acoplamiento de impedancia. Cuando alguno de estos componentes no tiene la misma impedancia, la eficiencia de transmisión se ve afectada.

Pérdida de retorno

La pérdida de retorno es otra forma de expresar la desadaptación. Es una medida logarítmica expresada en dB, que compara la potencia reflejada por la antena con la potencia con la cual la alimentamos desde la línea de transmisión *Pi*.

$$Return\ Loss\ (in\ dB) = 10 \log_{10} Pi/Pr$$

Aunque siempre existe cierta cantidad de energía que va a ser reflejada hacia el sistema, una pérdida de retorno elevada implica un funcionamiento inaceptable de la antena.

La interacción entre la onda que viaja desde el transmisor a la antena y la onda reflejada por la antena hacia el transmisor crea lo que se llama onda estacionaria, así que una forma alternativa de medir la desadaptación de impedancia es por medio de la Razón del Voltaje de la Onda Estacionaria (*Voltage Standing Wave Ratio (VSWR):*

$$Return\ Loss\ (in\ dB) = 20 \log_{10} (VSWR+1/VSWR-1)$$

En una línea de transmisión perfectamente acoplada, VSWR = 1.
En la práctica, tratamos de mantener una VSWR menor a 2.

Ancho de banda

El ancho de banda de una antena se refiere al rango de frecuencias F_H - F_L en el cual puede operar de forma correcta. Este ancho de banda es el número de hercios (Hz) para los cuales la antena va a cumplir ciertos requisitos como presentar una ganancia dentro de los 3 dB de la ganancia máxima, o un VSWR menor que 1.5.

El ancho de banda también puede ser descrito en términos de porcentaje de la frecuencia central de la banda:

$$Bandwidth = 100\ (F_H - F_L)/F_C$$

donde F_H es la frecuencia más alta en la banda, F_L es la frecuencia más baja, y F_C es la frecuencia central. De esta forma, el ancho de banda es constante respecto a la frecuencia. Si el ancho de banda fuera expresado en unidades absolutas de frecuencia, variaría dependiendo de la frecuencia central. Los diferentes tipos de antenas tienen diversas limitaciones de ancho de banda.

Directividad y Ganancia

La directividad es la habilidad de una antena de transmitir enfocando la energía en una dirección particular, o de recibirla de una dirección particular. Si un enlace inalámbrico utiliza ubicaciones fijas para ambos extremos, es posible utilizar la directividad de la antena para concentrar la transmisión de la radiación en la dirección deseada. En una aplicación móvil, donde el transceptor no está fijado a un punto, es imposible predecir dónde va a estar, y por lo tanto la antena debería radiar en todas las direcciones del plano horizontal. En estas aplicaciones se utiliza una antena omnidireccional. La ganancia no es una cantidad que pueda ser definida en términos de una cantidad física como vatios u ohmios: es un cociente sin dimensión. La ganancia se expresa con referencia a una antena estándar. Las dos referencias más comunes son la antena isotrópica y la antena dipolo resonante de media longitud de onda. La antena isotrópica irradia en todas direcciones con la misma intensidad. En la realidad esta antena no existe, pero provee un patrón teórico útil y sencillo con el que comparar las antenas reales. Cualquier antena real va a irradiar más energía en algunas direcciones que en otras. Puesto que las antenas no crean energía, la potencia total irradiada es la misma que una antena isotrópica. Toda energía adicional radiada en las direcciones favorecidas es compensada por menos energía radiada en las otras direcciones. La ganancia de una antena en una dirección dada es la cantidad de energía radiada en esa dirección comparada con la energía que podría radiar una antena isotrópica en la misma dirección alimentada con la misma potencia. Generalmente estamos interesados en la ganancia máxima, que es aquella en la dirección hacia la cual la antena está radiando la mayor potencia. Una ganancia de antena de 3dB comparada con una isotrópica debería ser escrita como 3dBi. El dipolo de media longitud de onda es un estándar útil a la hora de compararlo con otras antenas a una frecuencia, o sobre una banda estrecha de frecuencias. A diferencia de la isotrópica, es muy fácil de construir y a veces los fabricantes expresan la ganancia en referencia a la dipolo de media longitud de onda en lugar de la isotrópica. Una ganancia de antena de 3 dB comparada con una dipolo debería escribirse como 3 dBd. Puesto que la dipolo de media longitud de onda tiene una ganancia de 2,15 dBi, podemos calcular la ganancia dBi de cualquier antena sumando 2,15 a su ganancia dBd.

El método para medir la ganancia mediante la comparación de la antena bajo prueba con una antena estándar conocida, de ganancia calibrada, es conocido como técnica de transferencia de ganancia.

Patrón de Radiación

El patrón de radiación o patrón de antena describe la intensidad relativa del campo radiado en varias direcciones desde la antena a una distancia constante. El patrón de radiación es también de recepción, porque describe las propiedades de recepción de la antena.

El patrón de radiación es tridimensional, pero generalmente lo que se publica de este es una porción bidimensional del patrón tridimensional, en el plano horizontal o vertical.

Estas mediciones son presentadas en coordenadas rectangulares, o en coordenadas polares. La siguiente figura muestra el diagrama de radiación en coordenadas rectangulares de una antena Yagi de diez elementos. El detalle es bueno, pero se hace difícil visualizar el comportamiento de la antena en diferentes direcciones.

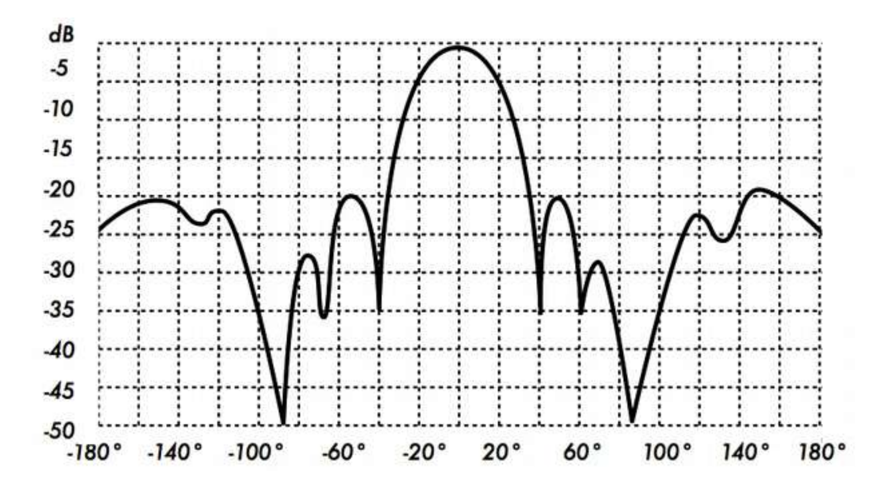


Figura ALT 7: Diagrama de radiación de una antena Yagi en coordenadas rectangulares

Los sistemas de coordenadas polares son usados casi universalmente.

En el gráfico de coordenadas polares, los puntos se obtienen por una proyección a lo largo de un eje que rota (radio) a una intersección con uno de varios círculos concéntricos que representan la ganancia correspondiente en dB, en referencia a 0dB en el extremo más externo del gráfico.

Esta representación hace más fácil de entender la distribución radial de la potencia de la antena.

En la Figura ALT 8 presentamos un diagrama de radiación en coordenadas polares de la misma antena Yagi de diez elementos.

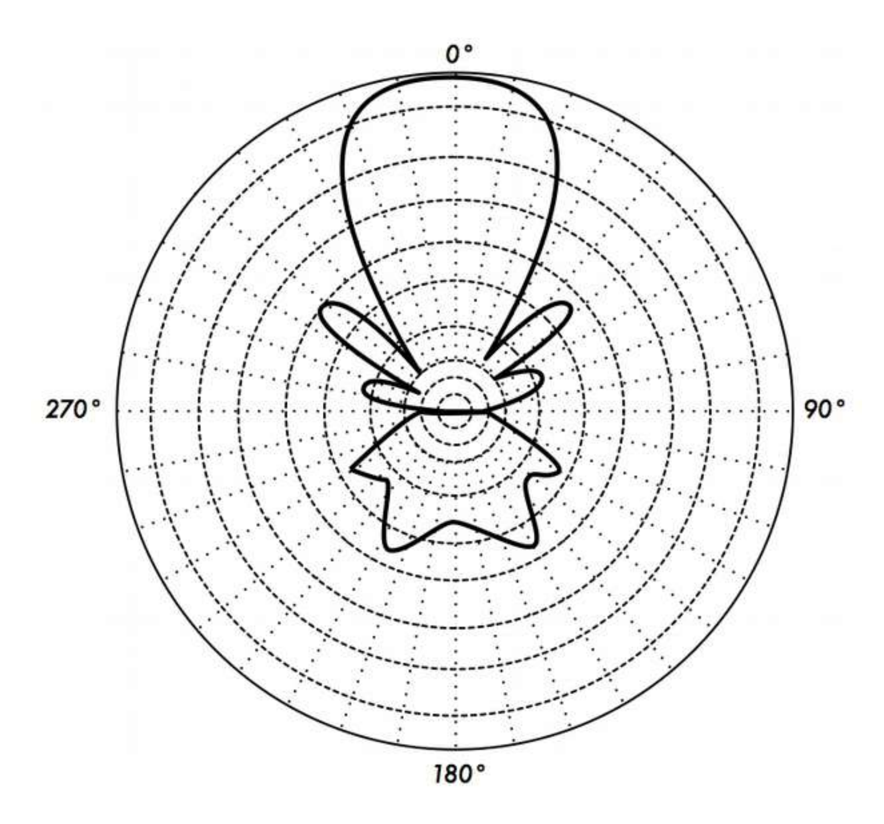


Figura ALT 8: Diagrama polar lineal de la misma antena Yagi

El patrón del campo que se observa cerca de la antena es diferente del más distante, que es el que nos interesa.

El campo lejano se llama también campo de radiación.

$r_{min} = 2d^2 / \lambda$

donde rmin es la distancia mínima desde la antena, d es la dimensión más grande de la antena y λ es la longitud de onda.

Ancho del haz

El ancho del haz de una antena usualmente se entiende como ancho del haz

a mitad de potencia. Se encuentra el pico de intensidad de radiación, luego se localizan los puntos de ambos lados de pico que representan la mitad de la potencia de intensidad del pico. La distancia angular entre los puntos de mitad potencia se define como el ancho del haz. La mitad de la potencia expresada en decibeles es de -3dB, por lo tanto algunas veces el ancho del haz a mitad de potencia es referido como el ancho del haz a 3dB. Generalmente se consideran tanto el anchos de haz vertical como horizontal.

Suponiendo que la mayoría de la potencia radiada no se dispersa en lóbulos laterales, la directiva, y por lo tanto la ganancia, es inversamente proporcional al ancho del haz: cuando el ancho del haz decrece, la ganancia se incrementa. Una antena de alta ganancia puede tener un ancho de haz de pocos grados y tendrá que ser apuntada muy cuidadosamente para no fallar el blanco. El ancho del haz se define por los puntos de la mitad de la potencia y a su vez determina el área de cobertura.

El área de cobertura se refiere al espacio geográfico "iluminado" por la antena y se define aproximadamente por la instersección del ancho del haz con la superficie terrestre. En una estación base es muy deseable maximizar el área de cobertura, pero a veces se debe recurrir al basculamiento de la antena sea mecánica o eléctricamente para poder darle al usuario un rendimiento semejante a la estación base, es decir, por debajo del ancho del haz de una antena no-basculada. Este basculamiento puede lograrse inclinando mecánicamente la antena, pero a menudo el haz puede ser dirigido cambiando la fase de la señal aplicada a los diferentes elementos de la antena en lo que se conoce como *basculamiento eléctrico*.

Lóbulos laterales (*sidelobes*)

Ninguna antena es capaz de irradiar toda la energía en una dirección preferida. Alguna energía se irá en otras direcciones. Estos pequeños picos se conocen como lóbulos laterales y se especifican en dB por debajo del lóbulo principal.

Nulos

En los diagramas de radiación de una antena, una zona nula es aquella en la cual la potencia efectivamente radiada está en un mínimo.

Un nulo a menudo tiene un ángulo de directividad estrecho en comparación al haz principal. Los nulos son útiles para varios propósitos tales como la supresión de señales interferentes en una dirección dada.

Polarización

La polarización se define como la orientación del campo eléctrico de una onda electromagnética. La polarización inicial de una onda de radio es determinada por la antena. La mayor parte de las antenas está polarizada vertical u horizontalmente.

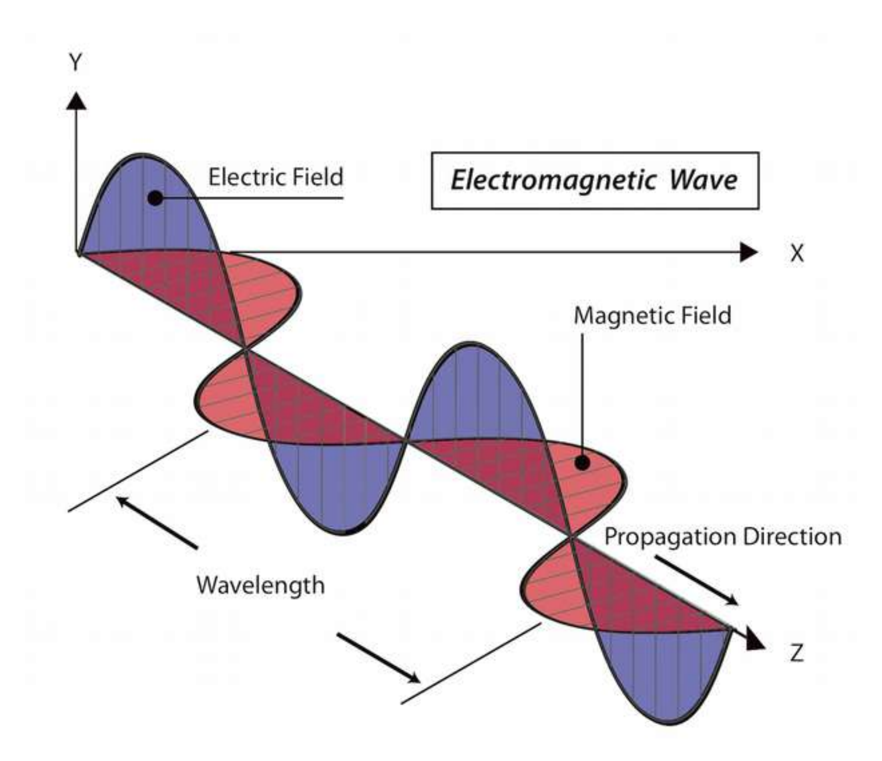


Figura ALT 9: El campo eléctrico es perpendicular al campo magnético y ambos son perpendiculares a la dirección de propagación

La polarización de las antenas transmisoras y receptoras deben coincidir o se produce una gran pérdida

Algunos sistemas modernos aprovechan la polarización enviando dos señales independientes a la misma frecuencia, separadas por la polarización.
La polarización se describe generalmente como una elipse. Dos casos especiales de polarización elíptica son la polarización lineal y la circular.
Con la polarización lineal, el vector del campo eléctrico se mantiene en el mismo plano todo el tiempo.

El campo eléctrico puede dejar la antena en una orientación vertical, horizontal o en algún ángulo entre los dos. La radiación polarizada verticalmente se ve ligeramente menos afectada por las reflexiones en el trayecto de la transmisión. Las antenas omnidireccionales siempre tienen una polarización vertical. Las antenas horizontales tienen menos probabilidad de captar interferencias generadas por el hombre, normalmente polarizadas verticalmente.

En la polarización circular el vector del campo eléctrico aparece rotando con un movimiento circular en la dirección de la propagación, haciendo una vuelta completa para cada ciclo de RF. Esta rotación puede ser hacia la derecha o hacia la izquierda. La elección de la polarización es una de las elecciones de diseño disponibles para el diseñador del sistema de RF.

Discordancia de polarización

Para transferir la máxima potencia entre una antena transmisora y una receptora, ambas antenas deben tener la misma orientación espacial y el mismo sentido de polarización.

Cuando las antenas no están alineadas o no tienen la misma polarización, habrá una reducción en la transferencia de potencia entre ambas antenas. Esto va a reducir la eficiencia global y las prestaciones del sistema.

Cuando las antenas transmisora y receptora están polarizadas linealmente, una desalineación física entre ellas va a resultar en una pérdida por discordancia de polarización, que puede ser determinada utilizando la siguiente fórmula:

$$Loss\ (dB) = 20 \log_{10}(\cos \theta)$$

donde θ es la diferencia en el ángulo de alineación entre las dos antenas.

Para 15° la pérdida es de aproximadamente 0,3 dB, para 30° perdemos 1,25 dB, para 45° perdemos 3 dB y para 90° tenemos una pérdida infinita.

Resumiendo, cuanto más grande la discordancia de polarización entre una antena transmisora y una receptora, más grande la pérdida.

En el mundo real, la pérdida debida a una discordancia en polarización de 90° es bastante grande pero no infinita. Algunas antenas como las Yagi o las antenas de lata, pueden rotarse 90° de forma sencilla para concordar con la polarización del otro extremo del enlace.

La polarización puede aprovecharse en un enlace punto-a-punto. Use una herramienta de monitoreo para observar la interferencia desde redes adyacentes, y rote una antena hasta que se minimice la señal recibida. Ponga el enlace en línea y oriente el otro extremo para concordar la polarización. Esta técnica puede ser utilizada a veces para construir enlaces estables, aún en medio ambientes con mucho ruido RF.

La discordancia de polarización puede aprovecharse para enviar dos señales diferentes en la misma frecuencia al mismo tiempo, duplicando de esta manera el caudal (*throughput*) del enlace. Algunas antenas especiales que tienen doble alimentación pueden emplearse para este propósito. Ellas tienen dos conectores RF que conectan a dos radios independientes. El caudal en la vida real es un poco más bajo que el doble del caudal de la antena sola, a causa de la inevitable interferencia de polarización cruzada.

Relación de ganancia adelante/atrás

A menudo es útil comparar la Relación de ganancia adelante/atrás de las antenas direccionales. Este es el cociente de la directividad máxima de una antena con relación a su directividad en la dirección opuesta. Por ejemplo, cuando se traza el patrón de radiación en una escala relativa en dB, la relación de ganancia adelante/atrás es la diferencia en dB entre el nivel de radiación máxima en la dirección hacia adelante y el nivel de radiación a 180 grados. Este número no tiene sentido para un antena omnidireccional, pero es bastante relevante cuando se construye un sistema con repetidores en los cuales la señal enviada de regreso (backward) va a interferir con la señal útil y debe ser minimizada.

Apertura de la antena

La "apertura" eléctrica de una antena receptora se define como la sección transversal de una antena parabólica que entregaría la misma potencia a una carga acoplada. Es fácil observar que una rejilla parabólica tiene una apertura muy similar a un paraboloide sólido. La apertura de una antena es proporcional a la ganancia.

Recíprocamente, la apertura es la misma para una antena transmisora.

Note que el concepto de apertura no se visualiza fácilmente en el caso de una antena de alambre en la cual el área física es insignificante.

En este caso la apertura de la antena debe derivarse a partir de la fórmula de la ganancia.

Tipos de antena

Una clasificación de las antenas puede basarse en:

Frecuencia y tamaño

Las antenas utilizadas para HF son diferentes de las antenas utilizadas para VHF, las cuales son diferentes de las antenas para microondas. La longitud de onda es diferente a diferentes frecuencias, por lo tanto las antenas deben ser diferentes en tamaño para radiar señales a la correcta longitud de onda.

En este caso estamos particularmente interesados en las antenas que trabajan en el rango de microondas, especialmente en las frecuencias de los 2.4 GHz y 5 GHz. A los 2.4 GHz la longitud de onda es 12,5 cm, mientras que a los 5 GHz es de 6 cm.

Directividad

Las antenas pueden ser omnidireccionales, sectoriales o directivas. Las antenas omnidireccionales irradian aproximadamente la misma seña alrededor de la antena en un patrón completo de 360.º

Los tipos más populares de antenas omnidireccionales son las dipolos y las de plano de tierra. Las antenas sectoriales irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados.

Las **direccionales** o **directivas** son antenas en las cuales el ancho del haz es mucho más angosto que en las antenas sectoriales. Tienen la ganancia más alta y por lo tanto se utilizan para enlaces a larga distancia

Algunos tipos de antenas directivas son la **Yag**i, la **biquad**, la de **bocina**, la **helicoidal**, la **antena patch**, el **plato parabólico**, y muchas otras.

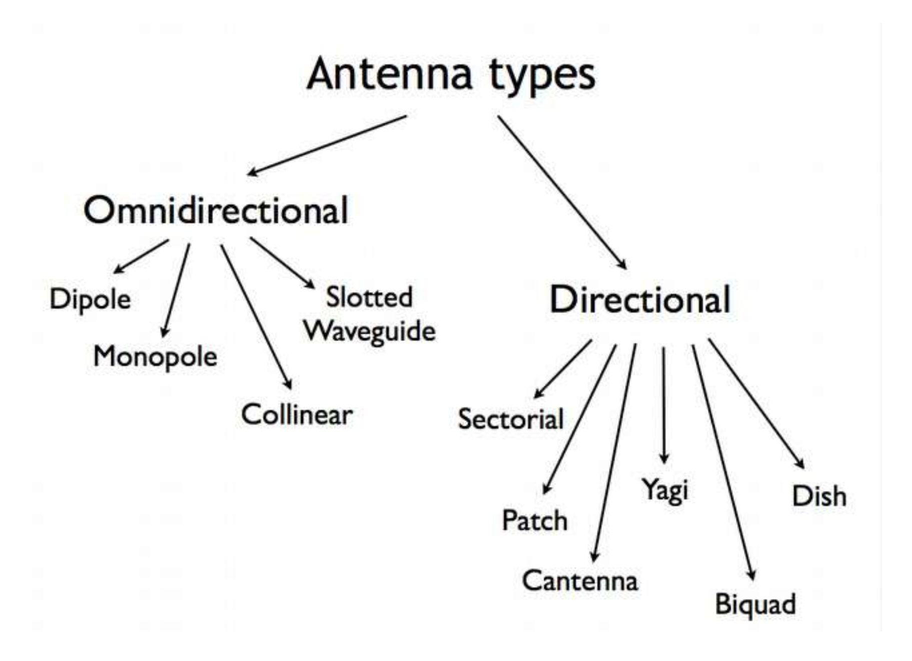


Figura ALT 10: Tipos de antenas

Construcción física

Las antenas pueden construirse de muchas formas diferentes, desde simples cables a platos parabólicos, o latas de café. Cuando consideramos antenas adecuadas para el uso en WLAN de 2.4 GHz se puede utilizar otra clasificación:

Aplicaciones

Los puntos de acceso tienden a hacer redes punto a multipunto, mientras que los enlaces remotos o troncales son punto a punto. Esto implica diferentes tipos de antenas para el propósito. Los nodos utilizados para accesos multipunto pueden utilizar tanto antenas omni las cuales irradian igualmente en todas direcciones, como antenas sectoriales que se enfocan en un área limitada. En el caso de los enlaces punto a punto, las antenas se usan para conectar dos lugares.

Las antenas directivas son la elección principal para esta aplicación.

A continuación presentamos una lista breve de los tipos de antenas para la frecuencia de 2.4 GHz proporcionando una descripción somera y una descripción básica sobre sus características.

Antena de 1/4 de longitud con plano de tierra

Esta antena es muy simple en su construcción y es útil para las comunicaciones cuando el tamaño, el costo y la facilidad de construcción son importantes. Esta antena se diseñó para transmitir una señal polarizada verticalmente. Consiste en un elemento de 1⁄4 de longitud onda como elemento activo y tres o cuatro elementos de 1⁄4 de longitud de onda inclinados de 30 a 45 grados hacia abajo. Este conjunto de elementos, denominados radiales, constituyen el plano de tierra.



Figura ALT 11: Antena de un cuarto de longitud de onda con plano de tierra

Esta es una antena simple y efectiva que puede captar una señal igualmente desde cualquier dirección. La ganancia de esta antena es del orden de los 2-4 dBi.

Antena Yagi-Uda

La antena Yagi, o más apropiadamente Yagi-Uda básica consiste en un cierto número de elementos rectos que miden, cada uno, aproximadamente la mitad de la longitud de onda. El elemento excitado o activo de una Yagi es el equivalente a una antena dipolo de media onda con alimentación central. En paralelo al elemento activo, y a una distancia que va de 0,2 a 0,5 longitud de onda en cada lado, hay varillas rectas o alambres llamados reflectores y directores, o, simplemente, elementos pasivos.

Un reflector se ubica detrás del elemento activo y es ligeramente más largo que media longitud de onda; un director se coloca en frente del elemento activo y es ligeramente más corto que media longitud de onda.

Una Yagi típica tiene un reflector y uno o más directores.

La antena propaga la energía del campo electromagnético en la dirección que va desde el elemento activo hacia los directores, y es más sensible a la energía electromagnética entrante en esta misma dirección.

Cuantos más directores tiene una Yagi, mayor la ganancia La siguiente es una foto de una antena Yagi con 5 directores y 1 reflector. Las antenas Yagi a menudo se encierran en una cúpula cilíndrica para protegerlas de la intemperie.

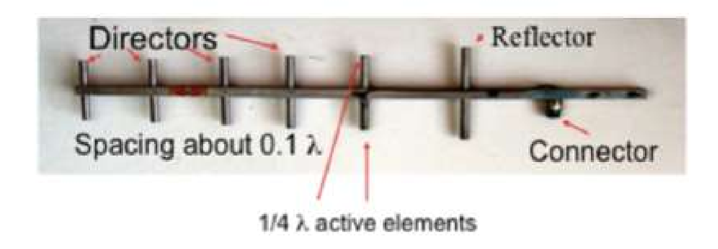


Figura ALT 12: Antena Yagi-Uda

Las antenas Yagi son utilizadas principalmente por los enlaces punto-a-punto, tienen una ganancia desde 10 a 20 dBi y un ancho de haz horizontal de 10 a 20 grados.

Antena bocina

El nombre de la antena bocina deriva de su apariencia característica acampanada o de cuerno. La porción acampanada puede ser cuadrada, rectangular, cilíndrica o cónica. La dirección de máxima radiación se corresponde con el eje de la campana.

Se puede alimentar sencillamente con una guía de onda, pero también puede hacerse con un cable coaxial y la transición apropiada.

A pesar de que es engorroso fabricar esta antena en casa, una lata cilíndrica de dimensiones adecuadas tiene características semejantes



Figura ALT 13: Antena bocina hecha con una lata de comida

Las antenas bocina se utilizan comúnmente como el elemento activo en una antena de plato. La bocina se coloca hacia el centro del plato reflector.

El uso de una bocina, en lugar de una antena dipolo, o cualquier otro tipo de antena en el punto focal del plato, minimiza la pérdida de energía alrededor de los bordes del plato reflector. A 2.4 GHz, una antena bocina simple hecha con una lata tiene una ganancia del orden de 10 dBi.

Plato parabólico

Las antenas basadas en reflectores parabólicos son el tipo más común de antenas directivas donde se requiere una gran ganancia.

La ventaja principal es que pueden construirse para tener una ganancia y una directividad tan grande como sea necesario.

La desventaja principal es que los platos grandes son difíciles de montar y podrían sufrir los efectos del viento. Los *radomes* (cobertura de material dielétrico para proteger la antena) pueden usarse para reducir los efectos del viento y para protección de la intemperie.



Figura ALT 14: Una antena plato sólida

Los platos de hasta un metro generalmente están hechos de material sólido. Frecuentemente se utiliza el aluminio por una ventaja de peso, su durabilidad y sus buenas características eléctricas. El efecto del viento se incrementa rápidamente con el tamaño del plato y se convierte en un problema severo. A menudo se utilizan platos que tienen una superficie reflectora constituida por una malla abierta. Éstos tienen una relación de ganancia adelante/atrás más pobre, pero son seguros de utilizar y sencillos de construir. Los materiales como el cobre, aluminio, bronce (latón), acero galvanizado y hierro son apropiados para una malla.

BiQuad

La antena BiQuad es fácil de armar y ofrece buena directividad y ganancia para las comunicaciones punto-a-punto. Consiste en dos cuadrados iguales de ¼ de longitud de onda como elemento de radiación y de un plato metálico o malla como reflector. Esta antena tiene un ancho del haz de aproximadamente 70 grados y una ganancia en el orden de 10-12 dBi. Puede ser utilizada como una antena única, o como un alimentador para un Plato Parabólico. Para encontrar la polarización: si observamos el frente de la antena, con los cuadrados colocados lado a lado, en esa posición la polarización es vertical.

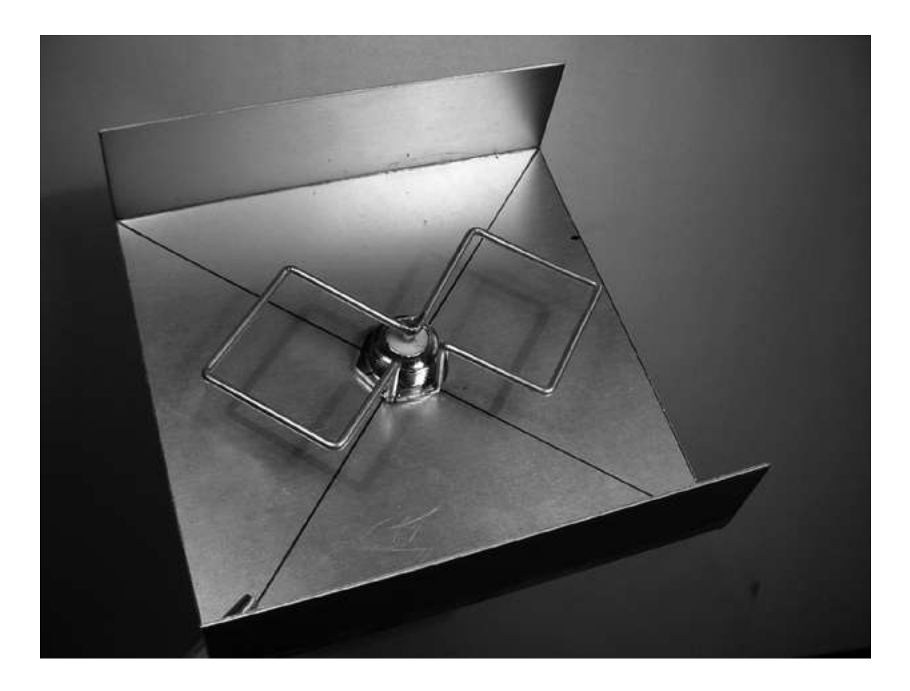


Figura ALT 15: Antena BiQuad.

Antenas Log Periodic

Estas antenas tienen una ganancia moderada en una banda de frecuencia amplia. Se usan a menudo en analizadores de espectro para hacer pruebas y también son populares como antenas receptoras de TV ya que cubren con eficiencia desde el canal 2 hasta el 14. Estas antenas se usan en espacios blancos (white spaces) que necesitan la capacidad para trabajar en canales muy diferentes.

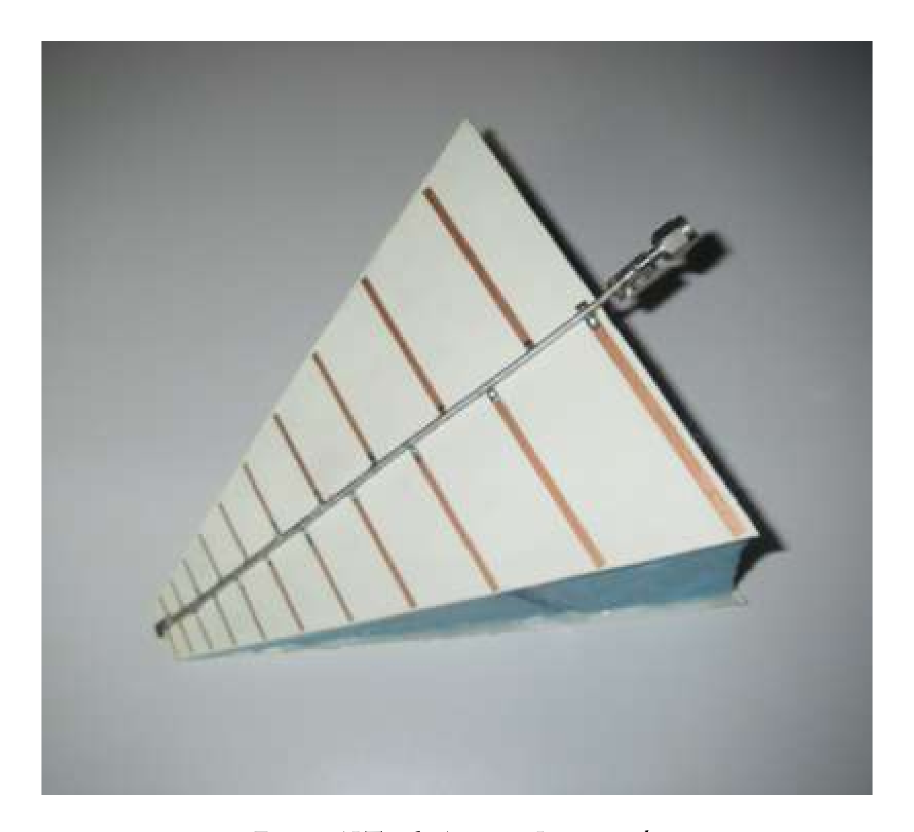


Figura ALT 16: Antena Log periodic

Otras Antenas

Existen muchos otros tipos de antenas y se crean nuevas siguiendo los avances tecnológicos.

Antenas de Sector o Sectoriales: son muy usadas en la infraestructura de telefonía celular y en general se construyen agregando una cara reflectora a una o más dipolos alimentadas en fase.

Su ancho de haz horizontal puede ser tan amplio como 180 grados, o tan angosto como 60 grados, mientras que el vertical generalmente es mucho más angosto. Las antenas compuestas pueden armarse con varios sectores para cubrir un rango horizontal más ancho (antena multisectorial).

Antenas Panel o Patch: son paneles planos sólidos utilizados para cobertura interior, con una ganancia de hasta 23 dBi.

Teoría de los reflectores

La propiedad básica de un reflector parabólico perfecto es que convierte una onda esférica irradiada desde un punto fuente ubicado en el foco, en una onda plana. Recíprocamente, toda la energía recibida en el plato desde una fuente distante se refleja en un punto único en el foco del plato. La posición del foco, o distancia focal, está dada por:

$$f = D^2 / 16\, c$$

donde **D** es el diámetro del plato y **c** es la profundidad de la parábola en su centro.

El tamaño del plato es el factor más importante ya que determina la ganancia máxima que puede lograrse a una frecuencia dada y el ancho del haz resultante. La ganancia y el ancho del haz obtenidos son dados por:

$$Ganancia = ((3.14\, D)^2 / \lambda^2)\, \eta$$

$$Ancho\ del\ haz = 70\, \lambda / D$$

donde **D** es el diámetro del plato y **η** es la eficiencia. La eficiencia es determinada principalmente por la efectividad de la iluminación del plato por el alimentador, pero también por otros factores. Cada vez que el diámetro del plato se duplica, la ganancia se cuadruplica o incrementa en seis dB. Si ambas estaciones duplican el tamaño de sus platos, la intensidad de la señal puede incrementarse en 12 dB, un aumento muy sustancial. Se puede estimar una eficiencia del 50% en una antena hecha a mano.

El coeficiente f / **D** (longitud focal/diámetro del plato) es el factor fundamental que define el diseño del alimentador para un plato. El coeficiente está directamente relacionado con el ancho del haz del alimentador necesario para iluminar el plato de forma efectiva. Dos platos del mismo diámetro pero con diferentes longitudes focales necesitan diferentes diseños del alimentador si ambos van a ser iluminados eficientemente. El valor de 0,25 corresponde al plato común de plano focal en el cual el foco está en el mismo plano que el aro del plato.

La iluminación óptima de un plato es un compromiso entre maximizar la ganancia y minimizar los lóbulos laterales.

Amplificadores

- Como mencionamos anteriormente las antenas no crean potencia. Ellas simplemente dirigen toda a potencia disponible en un patrón particular. Por medio de la utilización de un amplificador de potencia, usted puede usar energía DC para aumentar su señal disponible. Un amplificador se conecta entre el transmisor de radio y la antena, y tiene un cable adicional que se conecta a una fuente de energía. Existen amplificadores para trabajar a 2.4 GHz, que agregan varios vatios de potencia a su transmisión. Estos dispositivos detectan cuando el radio está transmitiendo, y empiezan a amplifican la señal. Cuando la transmisión termina se apagan otra vez. En recepción también agregan amplificación a la señal antes de enviarla al radio. Desafortunadamente, el simple hecho de agregar amplificadores no va a resolver mágicamente todos los problemas de nuestra red. No discutimos acerca de los amplificadores de potencia en profundidad en este libro, porque hay varios inconvenientes en el uso de los mismos:

- Son caros. Los amplificadores deben trabajar a relativamente grandes anchos de banda a 2.4 GHz, y deben tener una conmutación lo suficientemente rápida para trabajar con aplicaciones Wi-Fi. Estos amplificadores existen pero suelen costar varios cientos de dólares por unidad.

- No proveen direccionalidad adicional. Las antenas de alta no sólo mejoran la cantidad disponible de señal sino que tienden a rechazar ruido desde otras direcciones. Los amplificadores amplían ciegamente las señales deseadas y las interferencias, y pueden hacer que los problemas de interferencia sean peores.

- Los amplificadores generan ruido para otros usuarios de la banda. Debido al incremento de su potencia de salida, usted está creando una alta fuente de ruido para otros usuarios en la banda sin licenciamiento. Por el contrario, agregar ganancia de antena va a mejorar su enlace y puede bajar el nivel de ruido para sus vecinos.

- Utilizar amplificadores puede ser ilegal. Cada país impone límites de potencia para el espectro sin licenciamiento. Agregar una antena a una señal altamente amplificada, probablemente provoque que se excedan los límites legales.

Las antenas cuestan mucho menos que los amplificadores y se puede mejorar un enlace simplemente cambiando la antena de un extremo.
El uso de radios más sensibles y cable de buena calidad también ayuda mucho en los enlace inalámbricos de larga distancia.
Estas técnicas no suelen causar problemas a los otros usuarios de la banda, así que recomendamos seguirlas antes de añadir amplificadores.
Muchos fabricantes ofrecen versiones de alta potencia de sus radios WiFi para 2 y 5 GHz que ya tienen un amplificador incorporado. Estos son mejor que los amplificadores externos, pero no dé por sentado que es siempre mejor usar la versión de alta potencia, para muchas aplicaciones, una potencia estándar en combinación con una antena de alta ganancia es realmente mejor.

Diseños prácticos de antenas

El costo de las antenas de 2.4 GHz ha bajado considerablemente con la creciente popularidad de WiFi. Hay diseños innovativos que usan piezas más simples y menos materiales para lograr ganancias impresionantes minimizando la complejidad de manufactura. Desafortunadamente, la disponibilidad de buenas antenas es todavía limitada en algunas partes del mundo e importarlas puede ser costoso. Mientras que el diseño real de una antena puede ser un proceso propenso a errores, construirlas con componentes locales disponibles es bastante sencillo y puede ser muy divertido. En el **Apéndice A** llamado Construcción de Antenas les presentamos algunos diseños que se pueden construir con poco dinero.

Medidas de la antena

La medición precisa de las características de la antena requiere de instrumentos e instalaciones caros. Por lo tanto se recomienda obtener los valores de los parámetros directamente de las especificaciones de un fabricante de confianza. Para efectuar una medición precisa de la antena se necesita una cámara anecoica, de otra manera las reflexiones van a inducir falsas lecturas. El hielo afecta de alguna manera el rendimiento de todas las antenas y el problema se hace más serio a más altas frecuencias. La impedancia de espacio libre es de 377 ohmios. Si el aire que está en mayor contacto con la antena dipolo se reemplaza por hielo que tiene más baja impedancia que el aire entonces la adaptación de impedancia y los patrones de radiación de la antena cambian.

Estos cambios se incrementan a medida que la cantidad de hielo aumenta.
Los componentes de la antena están normalmente encerrados en una cúpula protectora de plástico (radome). Esto proporciona un espacio de aire entre los componentes y el hielo que se forme en la cúpula.
De esta manera, la impedancia más baja de la capa de hielo tendrá un efecto bajo en los radiadores.
De esta manera, la desadaptación de impedancia se reduce considerablemente, pero la distorsión de radiación subsiste (la desafinación reduce el ancho de banda utilizable de la antena).
Para un determinado espesor del hielo la desviación de los valores nominales de rendimiento empeora a medida que aumenta la frecuencia. En las zonas donde donde el hielo y la nieve son comunes es prudente instalar un radome completo sobre las parabólicas sólidas, usar paneles de antenas en lugar de reflectores de esquina y evitar las parabólicas de rejilla.



Figura ALT 17: Efecto del hielo en una parabólica de rejilla

REDES

6. REDES

Antes de adquirir equipos o decidirse por una plataforma de soporte físico, se debe tener una clara idea de la naturaleza de los problemas de comunicación que desea resolver. En realidad, si usted está leyendo este libro es porque necesita conectar sus redes de computadoras para compartir recursos y, en última instancia, acceder a Internet. El diseño de red que elija para su implementación debe concordar con los problemas de comunicaciones que está tratando de resolver.

¿Necesita conectar un lugar remoto a una conexión de Internet en el centro de su campus? ¿Es probable que su red crezca para incluir varios lugares alejados? ¿La mayoría de los componentes de su red van a estar instalados en ubicaciones fijas, o se va a expandir para incluir cientos de computadoras portátiles itinerantes y otros dispositivos?

En este capítulo, comenzaremos revisando los conceptos que definen TCP/IP, la principal familia de protocolos de red actualmente usados en Internet.

También examinaremos las opciones de hardware que probablemente formarán la capa física de su red TCP/IP y al final daremos ejemplos de configuraciones inalámbricas. Esto será una buena preparación para el capítulo sobre **Planificación e Instalación** más adelante.

TCP/IP hace referencia a una serie de protocolos que permiten mantener conversaciones en la Internet global. Al entender TCP/IP, usted podrá construir redes que puedan virtualmente alcanzar cualquier tamaño, y que a la postre formen parte de la Internet global.

Esta edición incluye una introducción a IPv6 que es el nuevo sistema de numeración de la Internet. Como es probable que usted vaya a instalar redes usando IPv6, es muy recomendable que se familiarice con su funcionamiento y sobre cómo trabajar junto con IPv4 que seguirá funcionando en Internet durante un buen tiempo todavía.

Introducción

Venecia, Italia es una ciudad fantástica para perderse. Las calles son simples pasos peatonales que cruzan las aguas de los canales en cientos de sitios, y nunca van en línea recta. Los carteros venecianos son de los más entrenados del mundo, especializados en hacer entregas a sólo uno o dos de los seis *sestieri* (distritos) de Venecia. Esto es necesario debido a la intrincada disposición de la antigua ciudad. Mucha gente encuentra que conocer la ubicación del sol y el agua es mucho más útil que tratar de encontrar el nombre de una calle en un mapa.

Imagine un turista que encuentra una máscara de papel maché como recuerdo y quiere enviarla desde la galería en S. Polo, Venecia, a su casa de Londres, en el Reino Unido. Esto parece una tarea ordinaria, o incluso trivial; pero veamos lo que pasa realmente.



Figura R1: Otro tipo de máscara en red

El artista, en primer lugar, empaca la máscara en una caja de cartón para despacharla a la casa del turista. Esta caja es recogida por un empleado de correos quien le añade una serie de formularios oficiales, y la envía a una oficina de acopio central para envíos internacionales. Después de algunos días, el paquete pasa la aduana italiana y está listo para un vuelo hacia el Reino Unido y llega a un sitio central de procesamiento de importaciones en el aeropuerto de Heathrow. Una vez que pasa la aduana, el paquete se envía al punto de distribución en Londres, y luego al centro de procesamiento local de correos de Camden, que es donde vive el turista. El paquete finalmente es transportado en un vehículo de reparto que tiene una ruta que lo llevará a la casa apropiada de la calle indicada, en Camden. Un miembro de la familia acepta el paquete y firma la hoja de entrega, y el turista finalmente disfrutará desempacando su máscara.

El empleado de la oficina de Camden ni sabe ni le interesa cómo llegar al *sestiere* de S.Polo en Venecia. Su trabajo es, simplemente, recibir los paquetes cuando llegan y expedirlos a la persona indicada en Camden. Igualmente, la compañía postal en Venecia no tiene por qué preocuparse de cómo llegar a la vecindad apropiada en Londres. Su trabajo es recoger los paquetes en la vecindad local y reenviarlos al próximo centro de acopio en la cadena de entrega.

El ejemplo anterior sirve para ilustrar cómo funciona el enrutamiento en Internet. Un mensaje es fragmentado en múltiples paquetes individuales, cada uno etiquetado con su origen y destino. El computador, entonces, envía estos paquetes a un enrutador (*router*), que decide dónde va a enviarlos a continuación. El enrutador sólo necesita recordar un número pequeño de rutas, por ejemplo, cómo llegar a la red local, la mejor ruta hacia algunas otras redes locales, y una ruta hacia una pasarela (*gateway*) que lo comunica al resto de Internet. Esta lista de posibles rutas se denomina tabla de enrutamiento (*routing table*). A medida que los paquetes llegan al enrutador, la dirección del destinatario es examinada y comparada con su tabla de enrutamiento interna. Si el enrutador no tiene una ruta explícita para el destino en cuestión, manda el paquete hacia la que más se le aproxime, que es, a menudo, su propia pasarela a Internet (a través de su ruta por defecto: *default route*). El próximo enrutador hace lo mismo, y así sucesivamente, hasta que el paquete finalmente llega a su destino.

Los paquetes de mercancía pueden ser enviados a través del sistema postal internacional sólo porque hemos establecido un sistema de direcciones estandarizado para este fin. Por ejemplo, la dirección del destinatario debe

estar escrita en el frente del paquete de forma legible, e incluir toda la información crítica (nombre del destinatario, calle, ciudad, país, código postal). Sin esta información, los paquetes o son devueltos al remitente, o se pierden en el sistema. Los paquetes de datos fluyen a través de la Internet global sólo en virtud de que hemos convenido sobre un sistema común de direcciones y un protocolo para el envío de los mismos. Estos protocolos de comunicación estándar hacen posible el intercambio de información a una escala global.

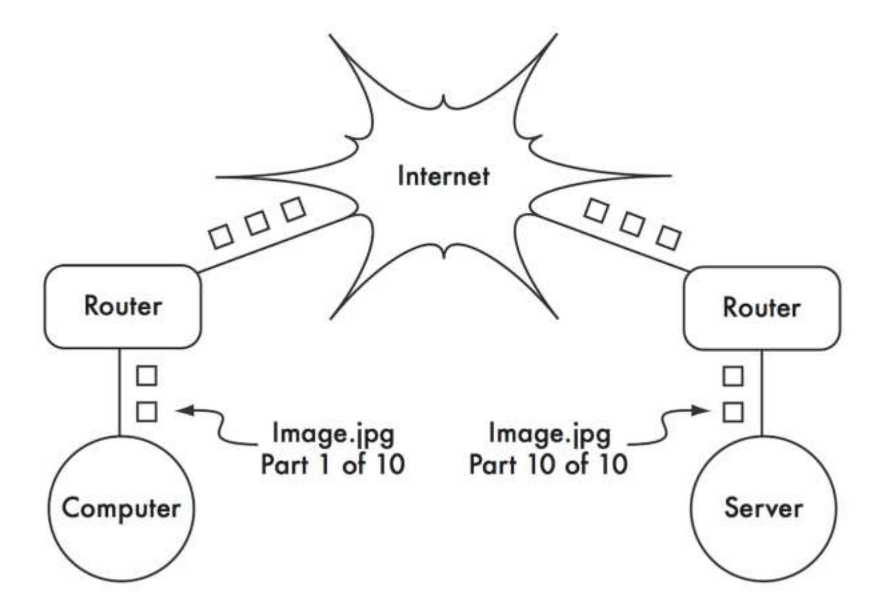


Figura R2: Red de Internet. Los paquetes se envían entre los enrutadores hasta que llegan a su destino final

Comunicaciones cooperativas

La comunicación es sólo posible cuando los participantes hablan una lengua común. Pero una vez que la comunicación se hace más compleja que una simple conversación entre dos personas, el protocolo se vuelve tan importante como la lengua.

Puede que toda la gente de un auditorio hable español, pero sin un conjunto de reglas establecidas para decidir quién tiene el derecho de usar el

micrófono, la comunicación de las ideas de una sola persona a la audiencia completa es casi imposible. Ahora, imaginemos un auditorio tan grande como el mundo, lleno de todos los computadores existentes. Sin un conjunto común de protocolos de comunicación para regular cuándo y cómo puede hablar cada computador, Internet sería un desastre caótico donde todas las máquinas tratan de hablar al mismo tiempo. Para resolver este problema se han desarrollado varios esquemas de comunicaciones entre los cuales, el más conocido es el modelo OSI.

El modelo OSI

El estándar internacional para Sistemas Abiertos de Interconexión, OSI (por su sigla en inglés: *Open Systems Interconnection*), se define en el documento ISO/IEC 7498-1, emanado de la International Standards Organization y la International Electrotechnical Comission. El estándar completo está disponible como publicación "ISO/IEC 7498-1: 1994", en http://standards.iso.org/ittf/PubliclyAvailableStandards/.

El modelo OSI divide el tráfico de la red en una cantidad de capas. Cada capa es independiente de las capas que la rodean y cada una se apoya en los servicios prestados por la capa inferior mientras que proporciona sus servicios a la capa superior. La separación entre capas hace que sea fácil diseñar una pila de protocolos (*protocol stack*) muy elaborada y confiable, tal como la difundida pila TCP/IP. Una pila de protocolos es una implementación real de un marco de comunicaciones estratificado. El modelo OSI no define los protocolos que van a usarse en una red en particular, sino que simplemente delega cada "trabajo" de comunicaciones a una sola capa dentro de una jerarquía bien definida. Mientras que la especificación ISO/IEC 7498-1 determina cómo deberían interactuar las capas, los detalles de la implementación real se dejan al fabricante. Cada capa puede implementarse en el hardware (es más común para las capas inferiores), o en el software. Siempre y cuando la interfaz entre capas se adhiera al estándar, los instaladores son libres de usar cualquier medio a su disposición para construir su pila de protocolos. Esto quiere decir que cualquier capa de un fabricante A puede operar con la misma capa de un fabricante B (suponiendo que las especificaciones relevantes se implementen e interpreten correctamente).

A continuación se presenta un breve bosquejo del modelo de redes OSI de siete capas.

Capa	Nombre	Descripción
7	Aplicación	La Capa de Aplicación es la capa con la que la mayoría de los usuarios tiene contacto; es el nivel en el que ocurre la comunicación humana. HTTP, FTP, y SMTP son todos protocolos de la capa de aplicación. El usuario se ubica por encima de esta capa, interactuando con la aplicación
6	Presentación	La Capa de Presentación tiene que ver con representación de datos, antes de que lleguen a la aplicación. Esto incluye codificación HTML, MIME, compresión de datos, comprobación del formato, ordenación de los bytes , etc.
5	Sesión	La Capa de Sesión maneja la sesión de comunicación lógica entre aplicaciones. RPC es un ejemplo de protocolo de la capa 5.
4	Transporte	La Capa de Transporte provee un método para obtener un servicio particular en un nodo de red específico. Algunos ejemplos de protocolos que operan en esta capa son TCP, UDP y SCTP. Algunos protocolos de la capa de transporte (como TCP), garantizan que todos los datos lleguen a destino y se reorganicen y entreguen a la próxima capa en el orden apropiado. UDP es un protocolo "no orientado a conexión" comúnmente usado para señales de video y audio de flujo continuo y no verifica la llegada de paquetes de datos.
3	Red	IP (el protocolo de Internet) es el más común de la Capa de Red. Esta es la capa donde ocurre el enrutamiento. Se encarga de transferir los paquetes desde la capa de enlace local a la de otras redes. Los enrutadores cumplen esta función en una red por medio de, al menos, dos interfaces de red, una en cada una de las redes que se van a interconectar. Cada nodo en Internet se accede a través de una dirección IP exclusiva. Otro protocolo crítico de Capa de Red es ICMP, un protocolo especial que proporciona varios mensajes necesarios para la adecuada operación de IP. Esta capa a menudo se denomina la Capa de Internet.
2	Enlace de Datos	Cada vez que dos o más nodos comparten el mismo medio físico (por ejemplo, varios computadores conectados a un concentrador (hub), o una habitación lleno de dispositivos inalámbricos que usan el mismo canal de radio), usan la Capa de Enlace de Datos para comunicarse. Los ejemplos más comunes de protocolos de enlace de datos son Ethernet, Token Ring, ATM, y los protocolos de redes inalámbricas (802.11a/b/g). La comunicación en esta capa se define como de enlace-local porque todos los nodos conectados a esta capa se comunican directamente entre sí. Esta capa también se conoce como capa de Control de Acceso al Medio (MAC en inglés). En redes Ethernet, los nodos se identifican por su dirección MAC. Esta es un número exclusivo de 48 bits asignado de fábrica a todo dispositivo de red.
1	Física	La Capa Física es la capa más baja en el modelo OSI, y se refiere al medio físico real en el que ocurre la comunicación. Este puede ser un cable CAT5 de cobre, un par de fibras ópticas, ondas de radio, o cualquier otro medio capaz de transmitir señales. Cables cortados, fibras partidas, e interferencia de RF son todos problemas de capa física.

Las capas de este modelo están numeradas del 1 al 7, con el 7 en el tope. Esto se hace para reforzar la idea de que cada capa está basada y depende de la capa de abajo. Imagine el modelo OSI como un edificio, con sus bases en la capa 1. Las próximas capas, como los pisos sucesivos, y el techo, como la capa 7. Si se remueve una sola capa, el edificio no se sostiene. De manera semejante, si se incendia el piso 4, nadie podría atravesarlo en ninguna de las dos direcciones.

Las primeras tres capas (Física, Enlace de Datos y Red) ocurren todas "en la red". Es decir, la actividad en estas capas va a estar determinada por la configuración de los cables, conmutadores, enrutadores y otros dispositivos semejantes. Un conmutador (*switch*) de red puede distribuir paquetes usando sólo direcciones MAC, así que necesita implementar sólo las capas 1 y 2. Un enrutador sencillo puede enrutar paquetes usando sólo sus direcciones IP, así que necesita implementar sólo las capas 1 a 3. Un servidor web o un portátil (laptop) ejecutan aplicaciones, así que deben implementar las siete capas. Algunos enrutadores avanzados pueden implementar desde la capa 4 en adelante lo que les permite tomar decisiones basadas en la información de alto nivel contenida en un paquete, como el nombre de un sitio web, o los adjuntos de un correo electrónico.

El modelo OSI es internacionalmente reconocido, y es considerado como el modelo de red definitivo y completo. Proporciona un esquema para los fabricantes e implementadores de protocolos de red que puede ser usado para construir dispositivos inter-operacionales en cualquier parte del mundo.

Desde la perspectiva de un ingeniero de redes, o una persona que trate de localizar una falla, el modelo OSI puede parecer innecesariamente complejo. En particular, la gente que construye o localiza fallas en redes TCP/IP rara vez se encuentra con problemas en las capas de Sesión o Presentación. Para la mayor parte de las implementaciones de redes, el modelo OSI puede ser simplificado en un conjunto menor de cinco capas.

El modelo TCP/IP

A diferencia del modelo OSI, el modelo TCP/IP no es un estándar internacional, y su definición varía. Sin embargo, es usado a menudo como un modelo práctico para entender y resolver fallas en redes Internet. La mayor parte de Internet usa TCP/IP, así que podemos plantear algunas premisas sobre las redes que las harán de más fácil comprensión. El modelo de redes TCP/IP describe las siguientes cinco capas:

Capa	Nombre
5	Aplicación
4	Transporte
3	Internet
2	Enlace de Datos
1	Física

En términos del modelo OSI, las capas cinco a siete quedan comprendidas en la capa superior (la Capa de Aplicación). Las primeras cuatro capas de ambos modelos son idénticas. Muchos ingenieros de redes consideran todo lo que está por encima de la capa cuatro como "sólo datos", que varían de aplicación a aplicación. Ya que las primeras tres capas son inter-operables para los equipos de casi todos los fabricantes, y la capa cuatro trabaja entre todos los anfitriones que usan TCP/IP, y todo lo que está por arriba de la capa cuatro es para aplicaciones específicas, este modelo simplificado funciona bien cuando se construyen o detectan fallas en redes TCP/IP. Vamos usar el modelo TCP/IP cuando hablemos de redes en este libro.

El modelo TCP/IP puede compararse a un mensajero que va a entregar una carta en un edificio de oficinas. Va a tener que interactuar primero con la calle (capa física), poner atención al tráfico de la misma (capa de enlace), doblar en los lugares correctos para conectarse con otras calles y llegar a la dirección correcta (capa Internet), ir al piso y oficina correcta (capa transporte), y finalmente encontrar el destinatario o recepcionista que pueda recibir la carta (capa de aplicación). Una vez entregada la carta, el mensajero queda libre. Las cinco capas pueden ser recordadas fácilmente usando la frase **F**avor **E**ntrar, **I**nmediatamente **T**omar el **A**scensor, para la secuencia de capas Física, Enlace de Datos, Internet, Transporte, y Aplicación, o en inglés "*Please Don't Look In The Attic*," que se usa por "*Physical / Data Link / Internet / Transport / Application*".

Los Protocolos de Internet

TCP/IP es la pila de protocolos más comúnmente usada en la Internet global. El acrónimo se lee en inglés *Transmission Control Protocol*, e *Internet Protocol*, respectivamente; pero en realidad se refiere a una familia completa de protocolos de comunicaciones relacionados.

TCP/IP también se conoce como grupo de protocolo Internet, y opera en las capas tres y cuatro del modelo TCP/IP. En la presente discusión nos concentraremos en la versión seis del protocolo IP (IPv6), ya que para el 2012 esta es la versión que se implementa en paralelo con la versión previa IPv4. En 2012 casi la mitad de los contenidos de Internet ofrecen un mejor acceso al usuario utilizando Ipv6. La versión anterior se explica en este capítulo también porque hay contenidos viejos o aplicaciones viejas (Skype 2012) todavía necesitan IPv4. Además, muchas redes con las que tendremos que interconectarnos van a tener la tecnología heredada de IPv4 por algunos años más todavía. Más allá de las diferencias en la longitud de las direcciones, IPv4 e IPv6 tienen semejanzas: ambas son protocolos de red no orientados a conexión que se apoyan en la misma capa de enlace de datos (WiFi, Ethernet, por ejemplo), y proporcionando servicio a los mismos protocolos de transporte (TCP, SCTP, UDP...). En este libro, cuando se escriba IP sin especificar la versión, va a significar que es aplicable a ambas versiones. Una red con pila de protocolos dual es una red que opera tanto en IPv6 como en IPv4. Se espera que estas redes duales sean la norma por lo menos hasta el 2020 cuando IPv6 será dominante.

Direccionamiento de IPv6

La dirección IPv6 es un número de 128 bits generalmente escrito como múltiples números hexadecimales. Para que los humanos puedan leerlo, se escribe en segmentos de 32 bits o cuatro números hexadecimales separados por dos puntos (:). El número hexadecimal debe escribirse en minúsculas, pero también puede hacerse en mayúsculas.
Un ejemplo de dirección IPv6 es:

2001:0db8:1234:babe:0000:0000:0000:0001

Esta dirección corresponde a:

2001	0db8	1234	babe	0	0	0	1

Como estas direcciones son bastante largas, es frecuente eliminar el cero inicial de cada segmento. Esta misma dirección también puede escribirse así:

2001:db8:1234:babe:0:0:0:1

La dirección puede todavía simplificarse sustituyendo un bloque de segmentos consecutivos de '0' por la forma abreviada '::'. Así, la misma dirección se transforma en:

2001:db8:1234:babe::1

Hay algunas direcciones IPv6 especiales:

- ::1 (ó 0000:00000:0000:0000:0000:0000:0000:0001) representa la dirección de *loopback*; es decir la del propio nodo mismo cuando quiere re-enviarse paquetes.
- :: (todos 'cero') es la dirección indeterminada que usa el nodo cuando no conoce su dirección global, por ejemplo al inicializar.

Prefijos IPv6

Los nodos del mismo enlace o red comparten el mismo prefijo IPv6 que se define como la parte más significativa de la dirección IPv6. En una LAN, el prefijo tiene normalmente 64 bits. Así que nuestra dirección 2001:db8:babe::1 se puede escribir 2001:db8:1234:babe::1/64 (el tamaño del prefijo se añade al final de la dirección después de una barra (/). Cuando se define el tamaño del prefijo, en realidad se divide la dirección en dos partes: el prefijo en sí mismo y el identificador de la interfaz (IID).

2001	0DB8	1234	babe	0	0	0	0
Prefijo				Identificador de Interfaz			

En una LAN o WLAN el tamaño del prefijo debe ser de 64 bits o algunos protocolos no van a trabajar correctamente. Todos los nodos de la misma LAN o WLAN normalmente comparten el mismo prefijo, pero sus IID deben ser exclusivas para evitar confusiones.
Siguiendo la analogía con la dirección postal de las ciudades, el nombre de la calles sería el prefijo, y el número de la casa el IID. El tamaño del prefijo puede ser diferente en enlaces que no son LAN o WLAN. La red misma es identificada por el prefijo sin ningún IID, pero especificando el tamaño. Por ejemplo: 2001:db8:1234:babe::/64

Direccionamiento IPv4

En una red IPv4, la dirección es un número de 32 bits, normalmente escrito como cuatro números de 8 bits expresados en forma decimal y separados por puntos. Ejemplos de direcciones IP son: 10.0.17.1; 192.168. 1.1; ó 172. 16. 5. 23.

Si se enumeraran todas las direcciones IP posibles, estas irían desde 0.0.0.0 hasta 255.255.255.255. Esto arroja un total de más de cuatro mil millones de direcciones IP posibles (255 x 255 x 255 x 255 = 4. 228. 250. 625). Sin embargo, muchas de estas están reservadas para propósitos especiales y no deberían ser asignadas a anfitriones.

Algunas direcciones IPv4 son especiales:

- 127.0.0.1 representa la dirección de *loopback*, parecida a ::1 para IPv6;
- 0.0.0.0 representa la dirección indeterminada (*unspecified address*), parecida a :: para IPv6.

Subredes IPv4

Aplicando una máscara de subred (también llamada máscara de red, o simplemente *netmask*, en inglés o incluso prefijo) a una dirección IPv4, se puede definir lógicamente tanto al anfitrión (*host*), como a la red a la que pertenece.

Tradicionalmente, las máscaras de subred se expresan utilizando formas decimales separadas por puntos, a la manera de una dirección IPv4. Por ejemplo, 255.255.255.0 sería una máscara común. Usted encontrará que esta notación se usa al configurar interfaces de redes, al crear rutas, etc. Sin embargo, las máscaras de subred se expresan más sucintamente utilizando notación CIDR que simplemente enumera la cantidad de bits en la máscara después de la barra (/). De esta manera, 225.225.225.0 puede simplificarse en /24. CIDR es la sigla en inglés de *Classless Inter-Domain Routing* (Enrutamiento entre dominios sin referencia a la clase), y está definida en RFC1518. Una máscara de subred determina el tamaño de una red dada. Al usar una máscara de red /24, hay 8 bits reservados para anfitriones: (32 bits en total —24 bits de máscara de red = 8 bits para anfitriones). Esto permite hasta 256 direcciones de anfitrión (28 = 256). Por convención, el primer valor se toma como la dirección de la red (.0 ó 00000000), y el último se toma como la dirección de difusión (.255 ó 11111111). Esto deja 254 direcciones libres para anfitriones en esta red.

Las máscaras de subred funcionan aplicando lógica AND al número IPv4 de 32 bits. En notación binaria, los bits “1” de la máscara indican la porción de la dirección de red, y los “0”, la porción de la dirección del anfitrión. Un AND lógico se efectúa comparando los dos bits. El resultado es “1” si los dos bits comparados son también “1”. De lo contrario, el resultado es “0”. A continuación exponemos todos los resultados posibles de la operación AND binaria entre dos bits.

Bit 1	Bit 2	Resultado
0	0	0
0	1	0
1	0	0
1	1	1

Para entender cómo una máscara de red se aplica a una dirección IPv4, primero convierta todo a binario. La máscara de red 255.255.255.0 en binario contiene veinticuatro bits “1”.

255 255 255 0

11111111.11111111.11111111.00000000

Cuando esta máscara de red se combina con la dirección IPv4 10.10.10.10, podemos aplicar el AND lógico a cada uno de los bits para determinar la dirección de la red.

10.10.10.10: 00001010.00001010.00001010.00001010

255.255.255.0: 11111111.11111111.11111111.00000000

10.10.10.0: 00001010.00001010.00001010.00000000

Esto da como resultado la red 10.10.10.0/24

Esta red comprende desde los anfitriones 10.10.10.1 hasta 10.10.10.254, con 10.10.10.0 como la dirección de red y 10.10.10.255 como la dirección de difusión.
Las máscaras de subred no están limitadas a octetos enteros. También se

pueden especificar máscaras de subred como 255.254.0.0 (ó /15 CIDR). Este es un bloque grande que contiene 131.072 direcciones, desde 10.0.0.0 hasta 10.1.255.255.

Podría continuar dividiéndose, por ejemplo, en 512 subredes de 256 direcciones cada una. La primera sería 10.0.0.0 - 10.0.0.255, luego 10.0.1.0 -10.0.1.255, y así sucesivamente, hasta 10.1.255.0 - 10.1.255.255. Alternativamente, podría ser dividido en dos bloques de 65.536 direcciones, u 8.192 bloques de 16 direcciones, o de muchas otras maneras diferentes. Incluso, podría dividirse en una combinación de diferentes tamaños de bloques, siempre y cuando ninguno se solape con otro, y que cada uno sea una subred válida cuyo tamaño sea una potencia de dos.

Aunque muchas máscaras de red son posibles, las más comunes son:

CIDR	Decimal	# de anfitriones
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256
/16	255.255.0.0	65 536
/8	255.0.0.0	16 777 216

Con cada decremento en el valor de CIDR, el espacio de direcciones IPv4 se duplica. Recuerde que en cada red hay dos direcciones IPv4 reservadas para las direcciones de red y de difusión.

Hay tres máscaras de red comunes que tienen nombres especiales. Una red / 8 (con una máscara de red de 255.0.0.0) define a una red Clase A.

Una /16 (255.255.0.0) es una Clase B, y una /24 (255.255.255.0) se llama Clase C. Estos nombres se usaban mucho antes de la notación CIDR, y se usan todavía con frecuencia por razones históricas.

Como vemos, es más fácil planificar con IPv6 que con IPv4.

Direcciones IP Globales

Las redes interconectadas deben concordar sobre un plan de direcciones IP para direcciones IPv6 e IPv4. Las direcciones IP deben ser exclusivas y, en general, no pueden usarse en sitios diferentes de Internet al mismo tiempo; de otra manera, los enrutadores no sabrían como dirigirles los paquetes.

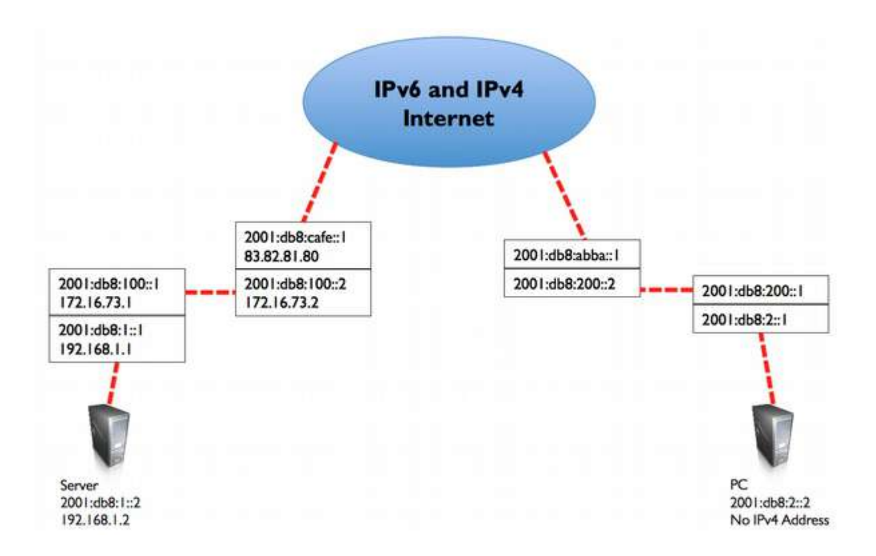


Figura R 3: Las direcciones IP exclusivas impiden la ambigüedad en el enrutamiento. Si el PC solicita una página web a 2001:db8:1::2, llegará al servidor correcto.

Con el fin de mantener las direcciones IP exclusivas y globalmente "enrutables" estas son asignadas por una autoridad central de asignación de números según un método consistente y coherente. Esto garantiza que las diferentes redes no utilicen direcciones duplicadas.

La autoridad central asigna grandes bloques de direcciones consecutivas a otras autoridades o a sus clientes. Los grupos de direcciones se denominan subredes o prefijos, como dijimos anteriormente. Y un grupo de direcciones relacionadas se llama espacio de direcciones.

Tanto IPv4 como IPv6 están administradas por la IANA (en inglés Internet Assigned Numbers Authority): http://www.iana.org/.

IANA ha dividido estos espacios de direcciones en grandes subredes, y estas subredes se han asignado a los cinco registradores regionales de Internet, RIR (Regional Internet Registrars) a los cuales se les ha concedido autoridad

sobre áreas geográficas grandes.
Las direcciones IP son asignadas y distribuidas por los RIR a los Proveedores de Servicio Internet o ISP (*Internet Service Provider*). El ISP luego asigna a sus clientes bloques más pequeños de direcciones IP según las necesidades. Prácticamente, todo usuario de Internet obtiene su dirección IP de un ISP.

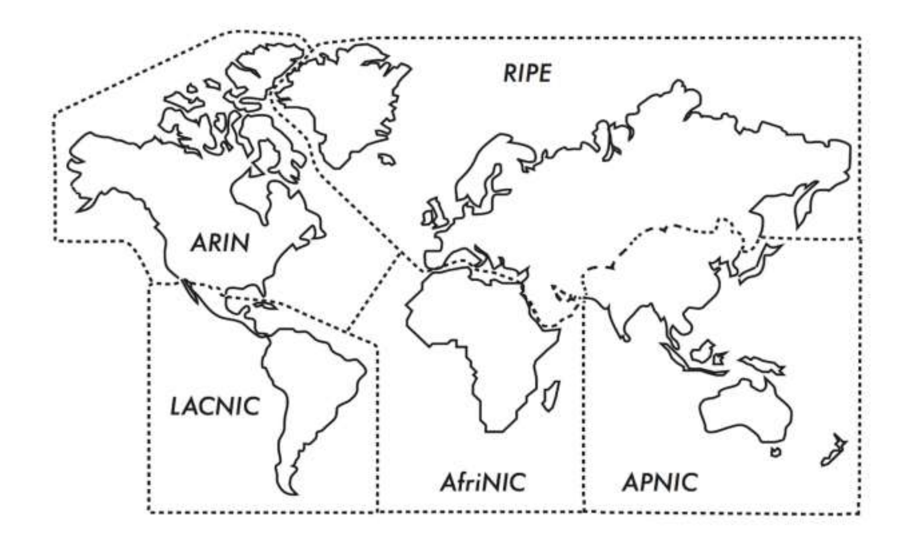


Figura R 4: La autoridad para asignar direcciones IP se delega en los cinco RIR

Los cinco RIR son:

1) African Network Information Centre (AfriNIC, http://www.afrinic.net)
2) Asia Pacific Network Information Centre (APNIC, http://www.apnic.net)
3) American Registry for Internet Numbers (ARIN, http://www.arin.net)
4) Regional Latin-American and Caribbean IP Address Registry (LACNIC, http://www.lacnic.net)
5) Réseaux IP Européens (RIPE NCC, http://www.ripe.net)

Su Proveedor de Servicios de Internet le asignará un espacio de direcciones IP enrutables globalmente, tomadas de las que le asigne el RIR. El sistema de registros se asegura de que las direcciones IP no se estén reutilizando en ninguna red de ninguna parte del mundo.

Una vez que se llegue a un acuerdo sobre las asignaciones de direcciones IP, es posible transmitir paquetes entre diferentes redes y participar en la Internet global. El proceso de mover paquetes entre las diferentes redes se conoce como enrutamiento.

Direcciones IP Estáticas

Una dirección IP estática es una dirección asignada que no cambia nunca. Las direcciones IP estáticas son importantes porque los servidores que las usan son alcanzables por los servidores DNS y comúnmente ofrecen servicios a otras máquinas (por ejemplo, servicio de correo electrónico, servidores web, etc.).

Los bloques de direcciones IP estáticas pueden ser asignados por su ISP, bajo pedido, o automáticamente, dependiendo de sus medios de conexión a Internet.

Direcciones IP Dinámicas

Las direcciones IP dinámicas son asignadas por un ISP para nodos no permanentes conectados a Internet, tales como computadores caseros conectados por discado, o una laptop conectada a un *hotspot* inalámbrico.
Las direcciones IP dinámicas pueden ser asignadas automáticamente usando el Protocolo Dinámico de Configuración de Anfitrión —*Dynamic Host Configuration Protocol* (DHCP), o el Protocolo Punto a Punto (PPP) dependiendo del tipo de conexión a Internet.

Un nodo que usa DHCP, en primer lugar le solicita a la red una dirección IP y automáticamente configura su interfaz de red. Las direcciones IP las puede asignar aleatoriamente su ISP a partir del bloque de direcciones que posee, o puede asignarse de acuerdo con una determinada política. Las direcciones IP asignadas por el DHCP son válidas por un período determinado (llamado período de adjudicación —*lease time*). El nodo debe renovar la adjudicación DHCP antes de su expiración. Al renovarla, el nodo puede recibir la misma dirección IP o una diferente dentro del grupo de direcciones disponibles.

Mientras que el DHCP funciona para IPv6 e IPv4, el IPv6 tiene otro mecanismo importante más usado para la asignación de direcciones que se llama Configuración Automática de Direcciones sin Estado o SLAAC por su sigla en inglés (Stateless Address Auto-Configuration); es usado por defecto en enrutadores y anfitriones que emplean IPv6.

No se necesita un servidor DHCP; el enrutador envía periódicamente mensajes de Anuncio del Router RA en todas las (W)LAN que contienen el prefijo de 64 bits que se ha de usar en esa (W)LAN; los anfitriones entonces generan su identificador de interfaz de 64 bits (normalmente un número aleatorio o un número basado en su dirección MAC, explicada más adelante) y construyen su dirección de 128 bits concatenando los 64 bits del prefijo del RA y la IID nueva recién creada.

Las direcciones dinámicas son muy populares entre los ISP, porque les permite usar menos direcciones IP que el número total de clientes que tienen.
Se necesita sólo una dirección por cada cliente que esté activo en un momento dado. Las direcciones IP globalmente enrutables son caras, y hay escasez de direcciones IPv4.

Asignar direcciones dinámicas le permite al proveedor de servicio ahorrar dinero, por lo que usualmente exigen un pago adicional a los clientes que deseen una dirección IP estática.

Direcciones IPv4 privadas

Hacia el año 2000 ya estaba claro que no habría suficientes direcciones IPv4 para todos; esta es la razón por la que el IPv6 fue concebido y desarrollado.
Pero se utilizó una solución temporal ya que la mayor parte de las redes privadas no necesitan asignación de direcciones públicas IPv4 globalmente enrutables para cada computador de la organización.
En particular, las direcciones de los computadores que no son servidores públicos no necesitan ser direccionables por la Internet pública.
Las organizaciones suelen usar direcciones IPv4 del conjunto del espacio de direcciones privado para las máquinas de una red interna.

Hoy en día existen tres bloques de espacio de direcciones privadas reservados por IANA:10.0.0.0/8, 172.16.0.0/12, y 192.168.0.0/16.

Estas están definidas en RFC1918.

Estas direcciones no son enrutables en la Internet, y suelen ser exclusivas solamente en el ámbito de una organización o grupo de organizaciones que haya escogido seguir el mismo esquema de numeración.
Esto significa que varias organizaciones no relacionadas pueden utilizar las mismas direcciones siempre y cuando nunca interconecten sus redes directamente.

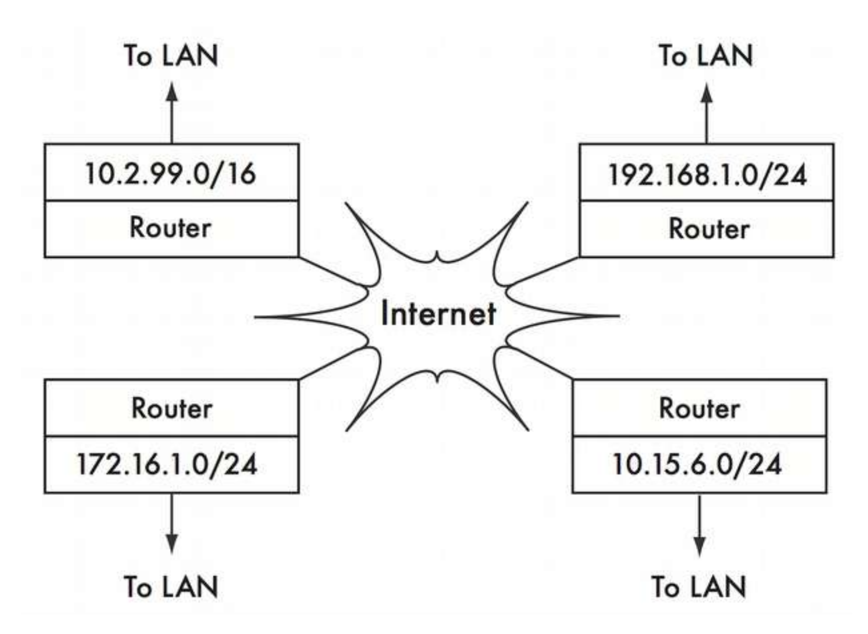


Figura R 5: Las direcciones privadas RFC1918 pueden ser usadas dentro de una organización y no son difundidas hacia la Internet global

Si usted alguna vez tiene la intención de interconectar redes privadas que usan espacio de direcciones RFC1918, asegúrese de no repetir direcciones en ninguna de las redes.

Por ejemplo, podría fragmentar el espacio de direcciones 10.0.0.0/8 en múltiples redes Clase B (10.1.0.0/16, 10.2.0.0/16, etc.).
Un bloque podría asignarse a cada red de acuerdo con su ubicación física (parte central del campus, primer grupo de oficinas, segundo grupo de oficinas, residencias estudiantiles, etc.).

Los/las administradores/as de red de cada ubicación pueden, a su vez, volver a fragmentar la red en múltiples redes Clase C (10.1.1.0/24, 10.1.2.0/24, etc.), o en bloques de cualquier otro tamaño lógico.

En el futuro, en el caso en que la red esté alguna vez conectada (sea físicamente, por enlace inalámbrico o VPN), todas las máquinas van a ser alcanzables desde cualquier punto en la red sin tener que volver a numerar los dispositivos de red.

Algunos proveedores de Internet pueden adjudicarles a sus clientes direcciones privadas como éstas, en lugar de direcciones públicas, a pesar de que hay serias desventajas.

Puesto que estas direcciones no pueden ser enrutadas en Internet, los computadores que las usan no son en verdad "parte" de Internet y no son directamente asequibles desde ella. Para poder conectarlos con Internet sus direcciones privadas deben ser convertidas en direcciones públicas. Este proceso de conversión se conoce como Traducción de Direcciones de Red (NAT, en inglés), y se ejecuta normalmente en la pasarela entre la red privada e Internet. Veremos más detalles de NAT más adelante en este capítulo. Como las direcciones IPv6 son muy numerosas, no hay necesidad de direcciones privadas en IPv6; sin embargo, hay Direcciones Locales Únicas (ULA en inglés) convenientes para redes sin conexión, como en los laboratorios, por ejemplo.

Descubriendo vecinos

Imagínese una red con tres computadores anfitriones: HA, HB, y HC. Estos usan las direcciones IP A, B y C, respectivamente. Estos anfitriones son parte de la misma subred/prefijo.

Para que dos anfitriones se comuniquen en una red local, deben conocer las direcciones MAC respectivas. Es posible configurar manualmente cada anfitrión con una tabla de mapeo desde una dirección IP a una dirección MAC, pero es más fácil descubrir de manera dinámica la dirección MAC de los vecinos usando el Protocolo de Descubrimiento del Vecino (NDP por el inglés *Neighbor Discovery Protocol*) en IPv6 y el Protocolo de Resolución de Direcciones, ARP (*Address Resolution Protocol*) en IPv4. NDP y ARP trabajan de forma parecida.

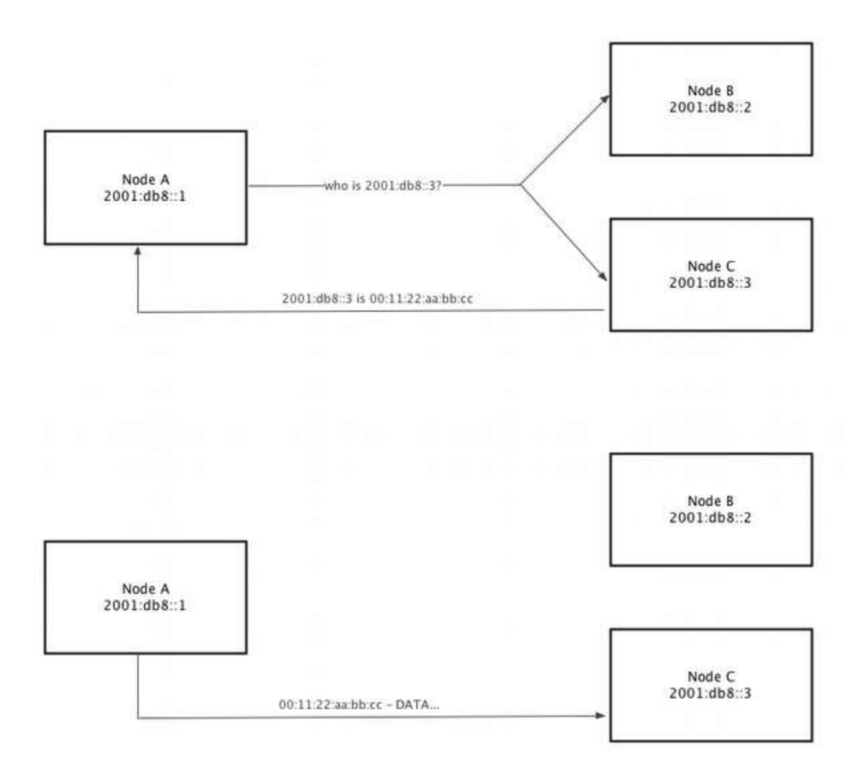


Figura R 6: el nodo IPv6 A, 2001:db8::1 necesita enviar datos a 2001:db8::3 en la misma red (prefijo 2001:db8::/64). Pero debe primero pedir la dirección MAC que le corresponde a 2001:db8::3.

Cuando se usa NDP, el nodo A manda a varios anfitriones la pregunta: ¿quién tiene la dirección MAC correspondiente a la dirección IPv6 2001:db8::3?

Cuando el nodo C ve la NS (*Neighbour Solicitatio*n en inglés) por su propia dirección IPv6, responde con su dirección MAC en un mensaje de NA (Neighbour Advertisement).

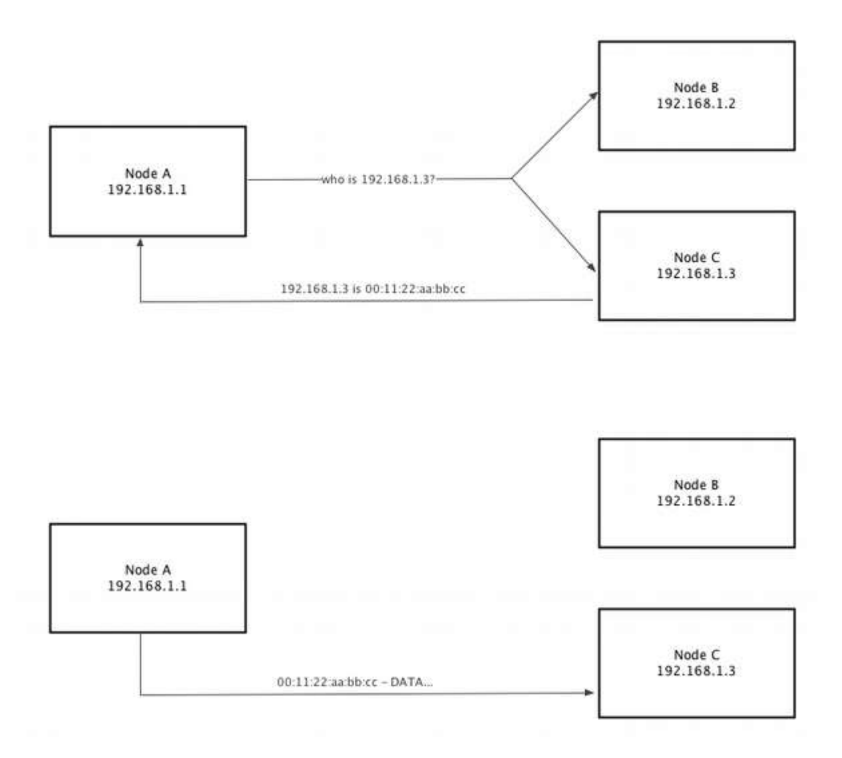


Figura R 7: EL nodo IPv4 A, 192.168.1.1, necesita enviar datos a 192.168.1.3 en la misma subred (192.168.1.0/24). Pero primero debe solicitar en la red entera la dirección MAC que le corresponde a 192.168.1.3

Cuando se usa ARP, el nodo A les manda a todos los anfitriones la pregunta: "¿Quién tiene la dirección MAC IPv4 192.168.1.3?"
Cuando el nodo C ve una petición ARP de su dirección IPv4, responde con su dirección MAC. El nodo B también ve la solicitud ARP, pero no va a responder porque no tiene la dirección 192.168.1.3. Esto es semejante a NDP en IPv6 excepto que un nodo IPv4 tiene una sola dirección.
ARP también envía la solicitud, lo que significa que todos los nodos IPv4 de la red la reciben, causando mayor utilización del CPU del anfitrión que el NDP de IPv6 que sólo envía la solicitud a algunos anfitriones.

Enrutamiento IP a los no vecinos

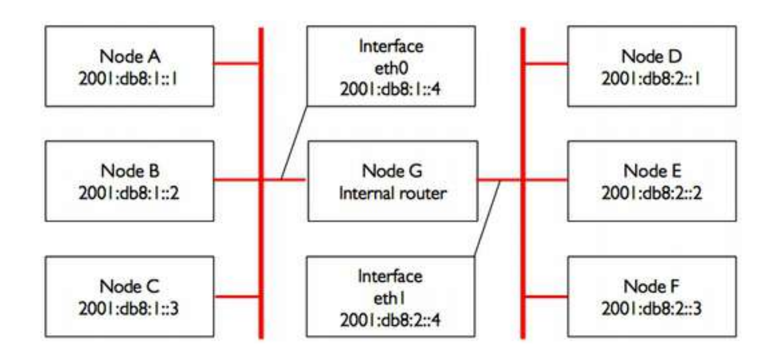


Figura R 8: Dos redes IPv6 separadas

Tomemos ahora otra red con tres nodos, D, E y F, con las direcciones IPv6 2001:db8:2::1, 2001:db8:2::2, y 2001:db8:2::3.
Esta es otra red /64, pero no en el mismo rango que la red de la izquierda en la figura anterior.
Los tres anfitriones pueden conectarse entre sí directamente: primero usando NDP para convertir la dirección IPv6 en dirección MAC y luego enviando los paquetes a esa dirección MAC.
Ahora añadimos el nodo G. Este nodo tiene dos tarjetas de red (también llamadas interfaces), cada una de las cuales está conectada a una de las redes. La primera tarjeta usa la dirección IPv6 2001:db8:1::4, en la interfaz eth0 y la otra usa la dirección 2001:db8:2:: en la eth 1.
El nodo G tiene ahora un enlace local a ambas redes y puede enviar paquetes entre ellas. Por esto recibe el nombre de enrutador o también pasarela (*gateway*).
¿Pero, que pasaría si A, B y C quieren conectarse con D, E y F? Necesitan saber que deben usar el nodo G por lo que deben añadir una ruta hacia la otra red a través de G. Por ejemplo, los anfitriones A-C añadirían una ruta estática a través de 2001:db8:1::4.
En Linux, esto se realiza con el comando:

ip -6 route add 2001:db8:2::/64 via 2001:db8:1::4

...y los anfitriones D-F añadirían:
ip -6 route add 2001:db8:1::/64 via 2001:db8:2::4

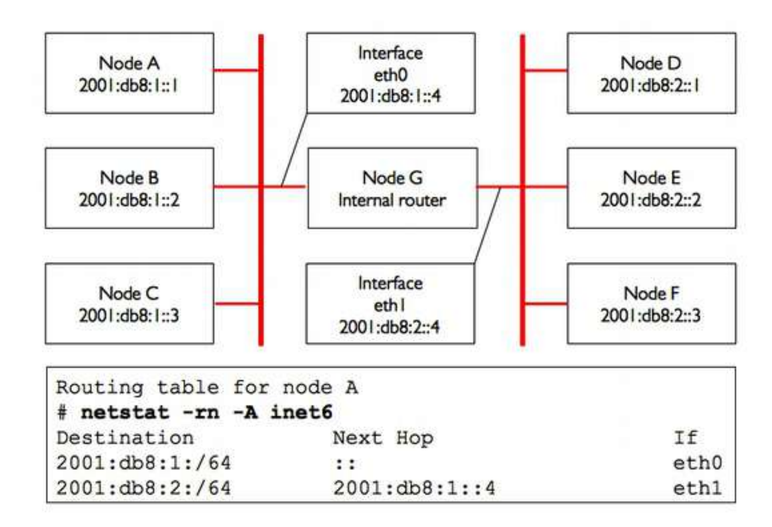


Figura R 9: El nodo G actúa como un enrutador entre las dos redes. Los otros anfitriones usan rutas estáticas

El resultado para el nodo A se muestra en la Figura R 9.

Nótese que la ruta se añade a través de la dirección IPv6 del anfitrión G que tiene un enlace local con la red respectiva.

El anfitrión A no podría agregar una ruta por 2001:db8:2::4, incluso compartiendo la misma máquina física con 2001:db8:1::4 (nodo G) ya que el IPv6 no es enlace local.

La dirección del próximo salto puede incluirse bien sea como una dirección global (2001:db8:2::4), o como una de enlace local (fe80::...); suele ser más fácil configurar una ruta estática con una dirección global.
En IPv6, el enrutador G también manda una solicitud y anuncios periódicos que contienen su propia dirección local, por lo tanto, todos los nodos que usan autoconfiguración sin estado o (DHCP) agregan automáticamente una ruta por defecto a través de la dirección local del enrutador, como se ilustra en la Figura R1 10.

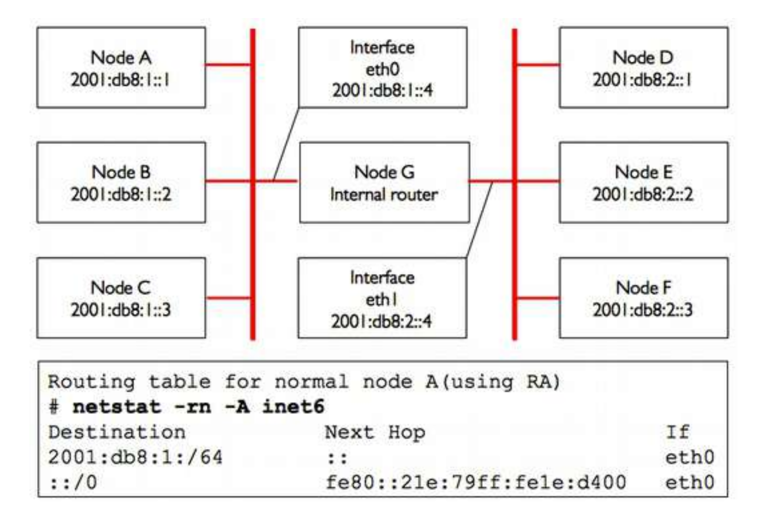


Figura R 10: EL nodo G funciona como enrutador entre las dos redes, los anfitriones usan la autoconfiguración de direcciones sin estado

Este es un ejemplo de enrutamiento muy sencillo donde el destino final está a un solo salto del origen. A medida que las redes se hacen más complejas, se necesitarán muchos saltos para alcanzar el destino final. Puesto que no sería práctico que cada máquina de Internet conociera la ruta hacia todas las demás, hacemos uso de una entrada de enrutamiento que se conoce como la ruta por defecto (o la pasarela por defecto). Cuando un enrutador recibe un paquete destinado a una red para la cual no se ha especificado una ruta, el paquete se remite a la pasarela por defecto. La pasarela por defecto suele ser la mejor ruta hacia el exterior de su red, usualmente en la dirección de su ISP.
Un ejemplo de un enrutador que usa una pasarela por defecto se muestra en la Figura R 11 donde se observa la tabla de enrutamiento (el conjunto de todas las rutas) del enrutador interno G que incluye las dos redes directamente conectadas 2001:db8:1::/64 y 2001:db8:2::/64, así como una ruta a todos los otros anfitriones de Internet ::/0.

Un nodo utiliza la ruta más específica; es decir, la ruta que presenta la mayor coincidencia hacia el destino final. En la Figura R 11, eth0 se usará para el destino 2001:db8:1::1 (longitud de coincidencia /64) en vez del menos específico ::/0 (longitud de coincidencia 0).

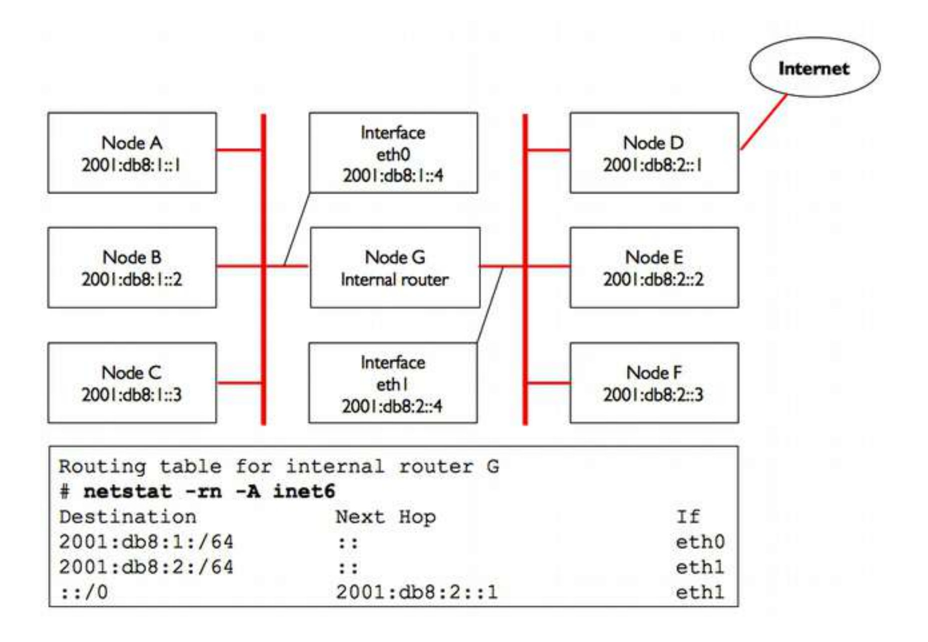
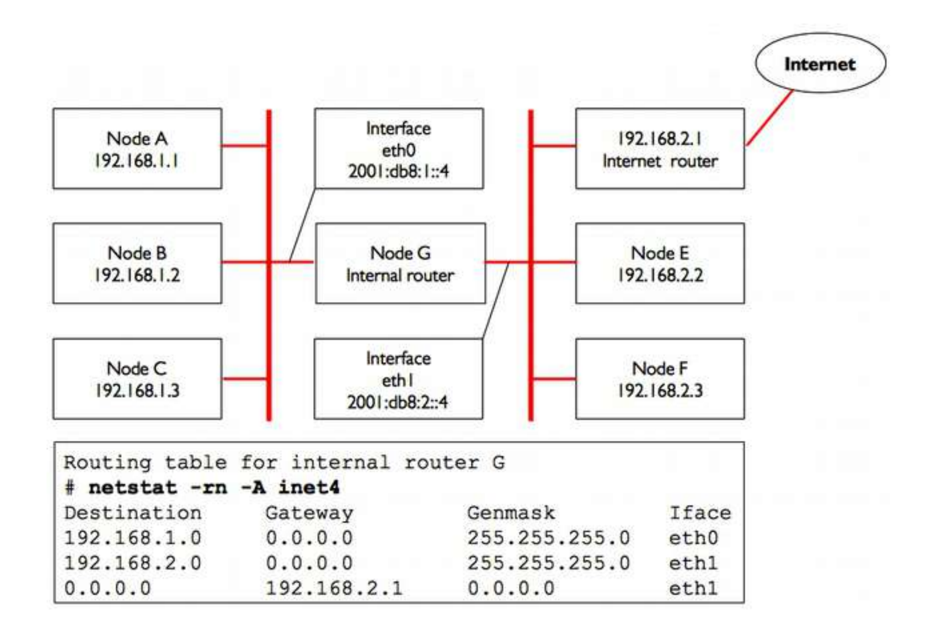


Figura R 11: El nodo G es el enrutador interno y usa el enrutador de Internet

Una ruta le dice al Sistema Operativo que la red buscada no está en la red inmediata de enlace local, y que debe reenviar el tráfico a través del enrutador especificado.
Si el anfitrión A quiere enviarle paquetes a F, debería primero mandarlos al nodo G. El nodo G entonces buscará a F en su tabla de enrutamiento, y verá que tiene conexión directa con la red del anfitrión F. Al final, G convierte la dirección MAC de F, y le entrega los paquetes.
Las rutas pueden ser actualizadas manualmente, o pueden reaccionar dinámicamente ante una falla de red, u otra eventualidad. Algunos ejemplos de protocolos populares de enrutamiento dinámico son RIP, OSPF, BGP.
Enseñar a configurar enrutamiento dinámico está más allá de los objetivos de este libro, pero para información adicional puede consultar los recursos del **Apéndice F**.

IPv4 se comporta exactamente de la misma forma como se ilustra en la Figura R 12.




```
Routing table for internal router G
# netstat -rn -A inet4
Destination     Gateway         Genmask          Iface
192.168.1.0     0.0.0.0         255.255.255.0    eth0
192.168.2.0     0.0.0.0         255.255.255.0    eth1
0.0.0.0         192.168.2.1     0.0.0.0          eth1
```

Figura R 12: El nodo G es el enrutador de Internet en esta red IPv4

Como dijimos antes, la mayor parte de las redes y la Internet son de doble pila (*dual-stack*) y todos los anfitriones y enrutadores tienen direcciones tanto IPv4 como IPv6; esto también significa que los nodos tendrán rutas para IPv4 e IPv6. Por ejemplo, el conjunto de todas las rutas en el nodo G de la figura anterior serán:

*# **netstat -rn -A inet6***

Destino	*Próximo Salto*	*Interfaz*
2001:db8:1:/64	*::*	*eth0*
2001:db8:2:/64	*::*	*eth1*
::/0	*2001:db8:2::1*	*eth1*

*# **netstat -rn -A inet4***

Destino	*Pasarela*	*Genmask*	*Interfaz*
192.168.1.0	*0.0.0.0*	*255.255.255.0*	*eth0*
192.168.2.0	*0.0.0.0*	*255.255.255.0*	*eth1*
0.0.0.0	*192.168.2.1*	*0.0.0.0*	*eth1*

Traducción de Direcciones de Red (NAT) para IPv4

Para poder contactar anfitriones en la Internet las direcciones privadas deben convertirse en direcciones IPv4 globales, públicamente enrutables.

Esto se logra por medio de una técnica que se llama Traducción de Direcciones de Red o NAT en inglés.
Un dispositivo NAT es un enrutador que modifica las direcciones de los paquetes además de reenviarlos.

En un enrutador NAT, la conexión a Internet usa una (o más) direcciones IPv4 globalmente enrutables, mientras que la red privada usa una dirección IPv4 de la gama de direcciones privadas RFC1918.
El enrutador NAT permite que la/las direcciones globales sean compartidas con todos los usuarios internos, que usan direcciones privadas.

Convierte los paquetes desde una forma de direcciones a otra, a medida que los paquetes lo atraviesan. Los usuarios/as, estos/as perciben como si estuvieran directamente conectados a Internet sin necesidad de software o controladores especiales.

Simplemente usan el enrutador NAT como la pasarela por defecto, y direccionan los paquetes, como lo harían normalmente.

El enrutador NAT traduce los paquetes dirigidos hacia afuera para que puedan usar las direcciones IPv4 globales a medida que salen de la red, y los vuelve a traducir cuando se reciben desde Internet.

La consecuencia más importante cuando se usa NAT es que una máquina en Internet puede tener dificultades en alcanzar a un servidor oculto detrás de un NAT a menos que se configuren reglas explícitas de redireccionamiento dentro del servidor NAT.

Las conexiones iniciadas desde el interior del espacio de direcciones privadas generalmente no presentan problemas, sin embargo, ciertas aplicaciones (como Voz sobre IPv4 y cierto software para VPN) pueden tener dificultades con el uso de NAT.

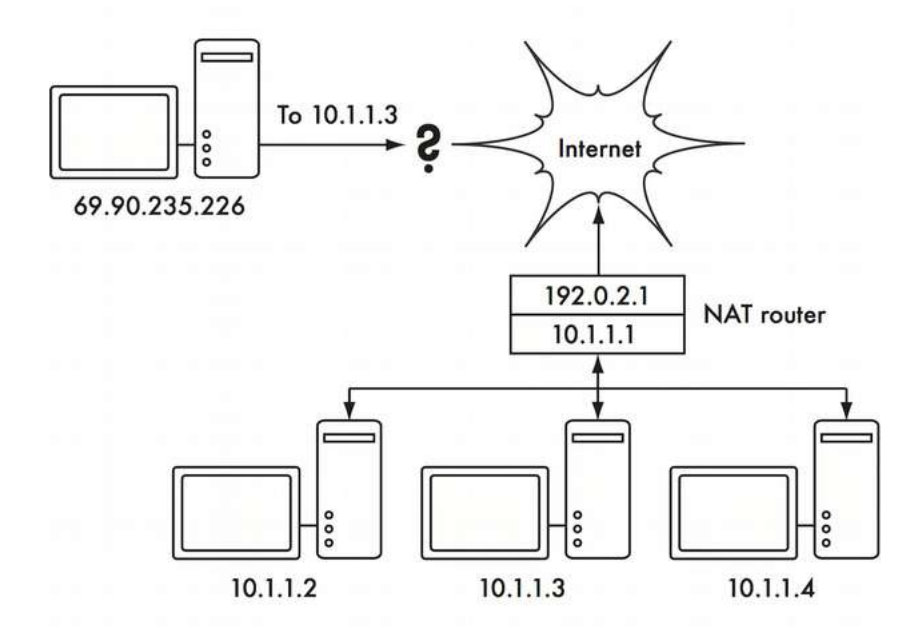


Figura R 13: NAT permite compartir una dirección única IPv4 con muchos anfitriones internos, pero puede dificultar el funcionamiento adecuado de algunos servicios

Dependiendo de su punto de vista, esto puede ser considerado un problema (puesto que hace que sea más difícil establecer una comunicación bidireccional), o una característica ventajosa, ya que en realidad le proporciona un cortafuego "gratis" a toda la organización. Las direcciones RFC1918 deberían filtrarse en el borde de su red para evitar que el tráfico RFC1918, de manera accidental, o malintencionada, entre o salga de su red. Mientras que NAT realiza algunas funciones de cortafuego, no es nunca un sustituto de uno verdadero ya que todos los ataques ocurren ahora cuando un usuario interno visita algún sitio web con contenidos peligrosos, llamados en inglés 'malware' (*malevolent software*).

Conjunto de Protocolos de Internet

Las máquinas en Internet usan el Protocolo de Internet (IP) para establecer contacto unas con otras, incluso cuando están separadas por múltiple máquinas intermediarias.

Hay un conjunto de protocolos que se ejecutan conjuntamente con IP y que proporcionan características tan importantes para las operaciones normales como el mismo protocolo IP. Cada paquete contiene un número de protocolo que identifica el protocolo utilizado.
Los protocolos más usados son el Transmission Control Protocol (TCP, número 6), el User Datagram Protol (UDP, número 17) y el Internet Control Message Protocol (ICPM, número 1 para IPv4 y 58 para IPv6). En conjunto, estos protocolos (y otros) se conocen como el Conjunto de Protocolos de Internet, o simplemente TCP/IP.

Los protocolos TCP y UDP introducen el concepto de número de puerto. Los números de puerto permiten que se ejecuten múltiples servicios bajo la misma dirección IP y que se puedan distinguir unos de otros. Cada paquete tiene un número de puerto de procedencia y de destino. Algunos números de puerto son estándares bien definidos que se usan para acceder a servicios bien conocidos, tales como servidores de correo electrónico y web.

Por ejemplo, los servidores web normalmente escuchan TCP en el puerto 80, para tráfico inseguro y en TCP, puerto 443 para tráfico encriptado/seguro. Los servidores de tiempo NTP escuchan en UDP, puerto 123; los servidores DNS escuchan en el puerto 53 con UDP y los de correo electrónico con SMTP en el puerto 25 con TCP.

Cuando decimos que un determinado servicio "escucha" en un puerto (como el 80), queremos decir que aceptará paquetes que usen su IP como dirección IP de destino, y 80 como el puerto de destino.

A los servidores normalmente les es indiferente la IP de procedencia o el puerto de procedencia, sin embargo, a veces se valen de esta información para establecer la identidad de la otra parte.

Cuando se envía una repuesta a estos paquetes, el servidor va a usar su propia IP como IP de procedencia, y 80 como puerto de procedencia. Cuando un cliente se conecta a un servicio, puede usar de su lado cualquier número de puerto de procedencia que no esté en uso, pero debe conectar con el puerto apropiado del servidor (p. ej. 80 para web, 25 para correo electrónico).

TCP es un protocolo orientado a sesión con entrega garantizada y ordenadas características de control de transmisión (como detección y mitigación de congestión en la red, retransmisión, reordenamiento y reensamblaje de paquetes, etc.).

UDP está diseñado para flujo de información sin conexión, y no garantiza entrega, ni ordenamientos específicos, pero puede ser más rápido, por lo que suele usarse para protocolos en tiempo real como los usados para temporización, voz y video.

El protocolo ICMP está diseñado para depuración y mantenimiento de la Internet. En lugar de números de puerto, usa tipos de mensaje, que también son números. Diferentes tipos de mensaje se usan para solicitar una simple respuesta de otro computador (solicitud de eco), para notificar al remitente de otro paquete sobre un posible lazo de enrutamiento (tiempo de transmisión excedido), o informarle al remitente que un paquete no ha podido enviarse debido a reglas de cortafuego u otros problemas (destino inalcanzable).

En este momento, usted debería tener un conocimiento sólido sobre cómo se intercomunican los computadores en la red, y de cómo fluye la información entre ellos. Examinemos ahora brevemente las herramientas físicas que implementan estos protocolos de red.

Herramientas físicas: *hardware*

Ethernet

Ethernet es el nombre del estándar más popular para conectar computadores en una Red de Área Local, LAN (*Local Area Network*). Se usa a menudo para conectar computadores individuales a Internet a través de un enrutador, módem ADSL, o dispositivo inalámbrico.

Sin embargo, si usted conecta un solo computador a Internet, puede que no use Ethernet. Su nombre viene del concepto físico de "éter", el medio que, según se creía antiguamente, transportaba las ondas luminosas a través del espacio libre. El estándar oficial se denomina IEEE 802.3.

El estándar Ethernet más común es el 100baseT, también llamado Fast Ethernet. Este define una tasa de datos de 100 megabits por segundo (de ahí el 100), sobre par trenzado (de ahí la T) con conectores modulares RJ-45 en el extremo.

La topología de red es una estrella con conmutadores o concentradores en el centro de cada estrella, y nodos finales (con dispositivos y conmutadores adicionales) en los extremos. Los servidores también se conectan usando Gigabit Ethernet con una tasa de 1 Gigabit por segundo.

Hoy en día, y cada vez más, Gigabit Ethernet reemplaza a Fast Ethernet en muchas redes a medida que la demanda para datos de video y de otras aplicaciones de alta velocidad se vuelve más relevante.

Direcciones de Control del Medio o Direcciones MAC

Cada dispositivo conectado a una red Ethernet o WiFi tiene una dirección MAC única asignada por el fabricante de la tarjeta de red. Su función es servir de identificador único que les permite a los dispositivos "hablar" entre sí. Sin embargo, el alcance de una dirección MAC se limita al dominio de difusión que va a estar definido por todos los computadores unidos a través de cables, concentradores, conmutadores y puentes, pero sin atravesar enrutadores ni pasarelas de Internet.

Las direcciones MAC nunca se usan directamente en la Internet y no son transmitidas entre enrutadores.

Las direcciones MAC para Ethernet y las redes WiFi IEEE 802.11 tienen 48 bits de longitud y lucen como: 00:1c:c0:17:78:8c ó 40:6c:8f:52:59:41; para esta última, los primeros 24 bits 40:6c:8f indican que Apple asignó esta dirección MAC.

Concentradores

Los concentradores Ethernet interconectan varios dispositivos Ethernet de par trenzado. Funcionan en la capa física (las más baja, la primera). Repiten las señales recibidas por cada puerto hacia el resto de los puertos. Los concentradores pueden, por lo tanto, ser considerados como simples repetidores.

Debido a su diseño, sólo uno de los puertos puede transmitir a la vez. Si dos dispositivos transmiten al mismo tiempo, las transmisiones se interfieren, y ambos se retiran para tratar de retransmitir los paquetes más tarde. A esto se le conoce como colisión, y cada anfitrión es responsable de detectar las colisiones que se producen durante la transmisión y de retransmitir sus propios paquetes cuando sea necesario.

Cuando en un puerto se detectan problemas, como un número excesivo de colisiones, algunos concentradores pueden desconectar ese puerto por un tiempo para limitar su impacto en el resto de la red. Mientras un puerto está desconectado, los dispositivos conectados con ese puerto no pueden comunicarse con el resto de la red.

Los concentradores están limitados respecto a su utilidad ya que pueden fácilmente convertirse en puntos de congestión en redes de mucho tránsito, razón por la cual hoy en día no se instalan en las redes. Pero es importante notar que un punto de acceso WiFi actúa como un concentrador en el lado del radio.

Conmutadores (*switches*)

Un conmutador es un dispositivo que funciona de manera muy parecida a un concentrador, pero proporciona una conexión dedicada (o conmutada) entre puertos.

En lugar de repetir todo el tráfico en cada puerto, el conmutador determina cuáles puertos se están comunicando directamente y los interconecta temporalmente. Puede haber varias conexiones temporales de puertos a la vez.

Los conmutadores proporcionan, en general, mejores prestaciones que los concentradores, especialmente en redes de mucho tráfico con numerosos computadores. No son mucho más caros que los concentradores y los reemplazan en muchas ocasiones.

Los conmutadores funcionan en la capa de enlace de datos (la segunda capa) puesto que interpretan y actúan sobre las direcciones MAC en los paquetes que reciben. Cuando un paquete llega a un puerto de un conmutador, éste determina la dirección MAC de procedencia asociada a ese puerto. Luego almacena esta información en una tabla MAC interna conocida como tabla CAM (*Content Addressable Memory*). El conmutador entonces busca la dirección MAC de destino en su tabla y transmite el paquete sólo al puerto que le corresponde. Si la dirección MAC de destino no se encuentra en la tabla, el paquete se manda a todas las interfaces conectadas esperando conseguir la MAC adecuada.

Concentradores versus Conmutadores

Los concentradores son considerados como dispositivos bastante elementales puesto que retransmiten de manera ineficiente todo el tráfico en cada puerto. Esta simplicidad acarrea tanto un defecto de rendimiento como un problema de seguridad. El rendimiento general es más lento ya que el ancho de banda disponible debe compartirse entre todos los puertos. Y, puesto que todo el tráfico es "visto" por todos los puertos cualquier anfitrión de la red puede fácilmente monitorear todo el tráfico de red.

Los conmutadores crean conexiones virtuales entre los puertos receptores y transmisores. Esto genera una mejor prestación porque se pueden hacer muchas conexiones virtuales simultáneamente. Los conmutadores más costosos pueden conmutar el tráfico por medio de inspección de los paquetes a niveles más altos (en la capa de transporte, o en la de aplicación), permitiendo la creación de VLAN, e implementando otras características avanzadas.

Un concentrador puede usarse cuando la repetición del tráfico en todos los puertos es deseable; por ejemplo, cuando usted quiere permitir explícitamente que una máquina de monitoreo vea todo el tráfico de la red. La mayoría de los conmutadores tienen un puerto de monitoreo que permite la repetición únicamente en un puerto designado específicamente para este propósito. Los concentradores solían ser más económicos que los conmutadores. Sin embargo, el precio de los conmutadores ha bajado considerablemente con el tiempo. Por lo tanto, las redes con concentradores deberían reemplazarse con las de conmutadores en la medida de lo posible.

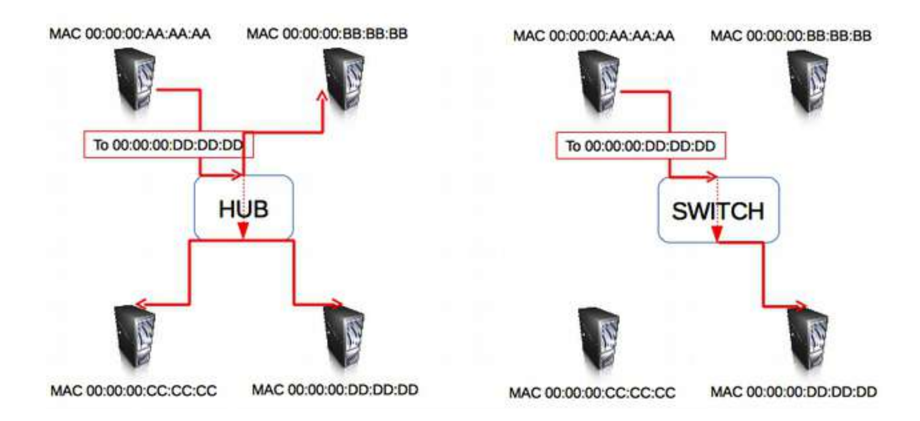


Figura R 14: Un concentrador simplemente repite todo el tráfico en cada puerto, mientras que un conmutador establece una conexión dedicada temporal entre los puertos que necesitan comunicarse

Tanto concentradores como conmutadores pueden ofrecer servicios administrados. Algunos de estos incluyen la capacidad de fijar la velocidad del enlace (10baseT, 100baseT, 1000baseT, duplex o half-duplex) en cada puerto, de disparar alarmas cuando hay incidentes en la red (como cambios

en la dirección MAC o paquetes malformados) y suelen incluir contadores en los puerto para calcular el ancho de banda. Un conmutador administrado que proporciona conteo de bytes de carga y descarga para cada puerto físico puede simplificar mucho la tarea del monitoreo de la red. Estos servicios están normalmente disponibles por SNMP, o se puede acceder a ellos por telnet, ssh, una interfaz web, o una herramienta especial de configuración.

Enrutadores y Cortafuegos

Mientras que los concentradores y los conmutadores proporcionan conectividad para un segmento de una red local, el trabajo de un enrutador es el de remitir paquetes entre diferentes segmentos de la red.

Un enrutador normalmente tiene dos o más interfaces físicas de red. Puede incluir interfaces para diferentes tipos de medios de red tales como Ethernet, WiFi, fibra óptica, DSL, o discado (*dial-up*). Los enrutadores pueden ser dispositivos dedicados de hardware, o pueden construirse a partir de un PC estándar con múltiples tarjetas de red y software apropiado.

Los enrutadores se encuentran en el borde de dos o más redes. Por definición, tienen una conexión con cada red, y en tanto máquinas de borde pueden asumir otras responsabilidades además del enrutamiento. Muchos enrutadores tienen capacidad de cortafuego que proporciona un mecanismo para filtrar o redirigir paquetes que no cumplen con las exigencias de seguridad o de políticas de acceso. También pueden suministrar servicios NAT para IPv4.

Los enrutadores varían considerablemente en precios y prestaciones. Los más económicos y menos versátiles son dispositivos simples de hardware dedicado, a menudo con función de NAT utilizada para compartir una conexión a Internet entre pocos computadores. Hay marcas bien conocidas como Linksys, D-Link, Netgear.

El siguiente nivel es un enrutador de software, que consiste en un sistema operativo en un PC estándar con múltiples interfaces de red. Los sistemas operativos estándares como Microsoft Windows, Linux y BSD tienen, todos ellos, la capacidad de enrutar, y son mucho más versátiles que los dispositivos de hardware más baratos. Esto se conoce como Compartición de Conexión a Internet. Sin embargo, presentan el mismo problema que las PC convencionales: alto consumo de energía, gran número de piezas muy complejas y poco confiables y configuración más engorrosa.

Los dispositivos más costosos son enrutadores dedicados de altas prestaciones, fabricados por compañías como Cisco y Juniper. Suelen ofrecer mejor rendimiento, más características, y mayor confiabilidad que los enrutadores basados en software en PC. También es posible comprar apoyo técnico y contratos de mantenimiento para estos dispositivos.

La mayor parte de los enrutadores modernos ofrecen posibilidades de monitorear y grabar remotamente el rendimiento, normalmente a través de SNMP (*Simple Network Managment Protocol*). Sin embargo, algunos de los dispositivos más sencillos no tienen esta característica.

Otros equipos

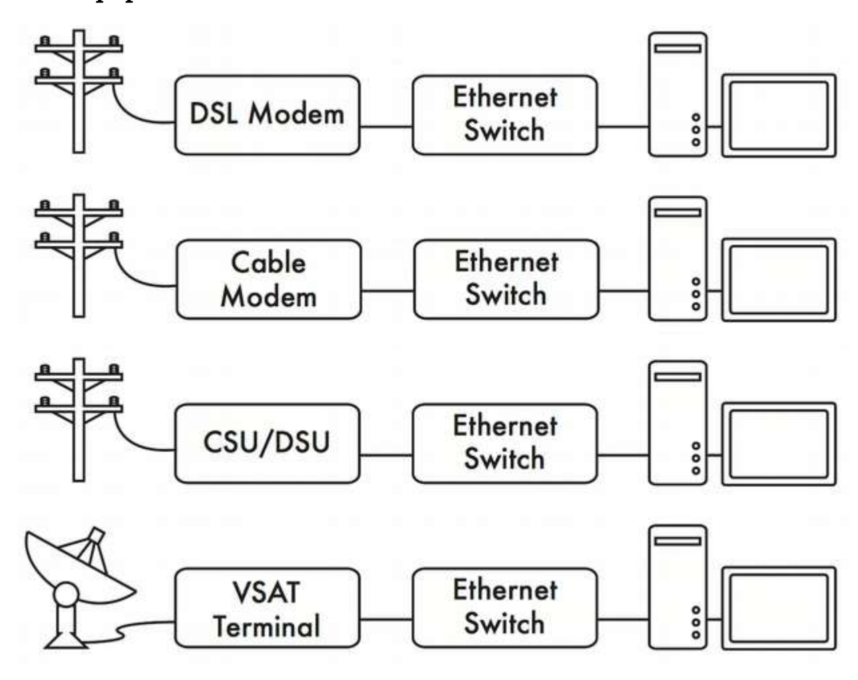


Figura R 15: Muchos módems DSL, módems para cable, CSU/DSU, puntos de acceso inalámbricos, y terminales VSAT terminan en un conector Ethernet

Cada red física usa un equipo terminal específico. Por ejemplo, las conexiones VSAT consisten en una antena parabólica conectada a un terminal que, o bien va enchufado a una tarjeta dentro de la PC, o termina en una conexión Ethernet estándar. Las líneas DSL utilizan un módem DSL

que hace puente entre la línea telefónica y un dispositivo local, sea una red Ethernet, o un único computador a través de USB. Los módems de cable hacen puente entre los sistemas de Tv por cable a Ethernet o a una interfaz interna del PC. Las líneas estándares de discado usan módems para conectar el computador al teléfono, normalmente a través de una tarjeta enchufable o de un puerto serial. Y también hay diferentes tipos de equipo de red inalámbrico que se conectan con una variedad de radios y antenas, pero casi todos terminan en un conector Ethernet.

La funcionalidad de estos dispositivos puede variar significativamente de acuerdo con el fabricante. Algunos proporcionan mecanismos de monitorear el rendimiento, mientras que otros no. Puesto que su conexión a Internet, en última instancia procede de su ISP, usted debería seguir las recomendaciones que le den respecto a la selección de equipos que hagan puente entre la red de su ISP y su propia red Ethernet.

Armando el conjunto

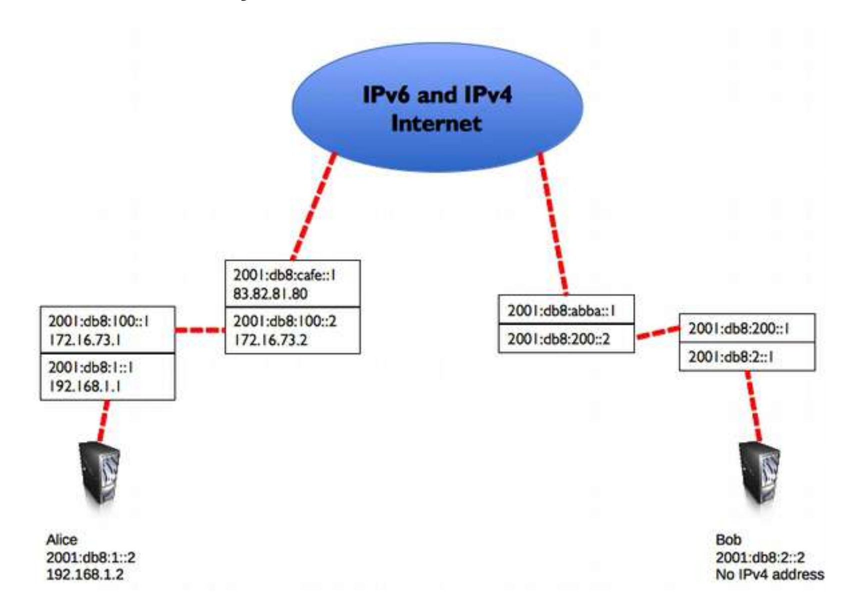


Figura R 16: Red de Internet. Cada segmento de red tiene un enrutador con dos direcciones IP estableciéndose un "enlace local" a dos redes diferentes. Los paquetes son reenviados entre los enrutadores hasta que llegan al destino final

Una vez que todos los nodos de la red tienen una dirección IP, pueden enviar paquetes de datos a cualquier otro nodo. Mediante el enrutamiento y el reenvío, esos paquetes pueden llegar a nodos en redes que no están conectadas físicamente con el nodo original. Este proceso describe mucho de lo que "sucede" en Internet.

En el ejemplo se puede ver el camino que toman los paquetes cuando Alice habla con Bob utilizando un servicio de mensajería instantánea. Cada línea punteada representa un cable Ethernet, un enlace inalámbrico, o cualquier otro tipo de red física.

El símbolo de la nube es usado comúnmente para "La Internet", y representa cualquier número de redes IP involucradas. Ni Alice ni Bob necesitan preocuparse de cómo operan esas redes, siempre que los enrutadores remitan el tráfico IP hasta el destino final. Si no fuera por los protocolos de Internet y la cooperación de todos en la red, este tipo de comunicación sería imposible.

En la figura descrita, Alice tiene un sistema de doble pila con direcciones IPv4 e IPv6, mientras que Bob tiene solamente direcciones IPv6: se comunicarán usando IPv6 que es la versión de IP que comparten.

Diseño de la red física

Puede parecer raro que hablemos de la red "física" cuando construimos redes inalámbricas. Después de todo, ¿dónde está la parte física de la red? En estas redes, el medio físico que utilizamos para la comunicación es, obviamente, la energía electromagnética. P
ero en el contexto de este capítulo, la red física se refiere al tema prosaico de dónde poner las cosas.
¿Cómo va a organizar el equipo de forma que usted pueda contactar a sus clientes inalámbricos? Sea que deba llegar hasta una oficina en un edificio o extenderse a lo largo de muchos kilómetros, las redes inalámbricas se organizan naturalmente en estas tres configuraciones lógicas: enlaces punto a punto, enlaces punto a multipunto, y nubes multipunto a multipunto.
Si bien las diferentes partes de su red pueden aprovechar las tres configuraciones, los enlaces individuales van a estar dentro de una de esas topologías.

Punto a punto

Los enlaces punto a punto generalmente se usan para conectarse a Internet donde el acceso no puede hacerse de otra forma. Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder a ella.

Por ejemplo, una universidad puede tener una conexión VSAT dentro del campus, pero difícilmente podrá justificar otra conexión de la misma índole para un edificio importante fuera del campus. Si el edificio principal tiene una visión libre de obstáculos al lugar remoto, una conexión punto a punto puede ser utilizada para unirlos. Ésta puede complementar o incluso remplazar enlaces de discado existentes. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto confiables que excedan los treinta kilómetros.

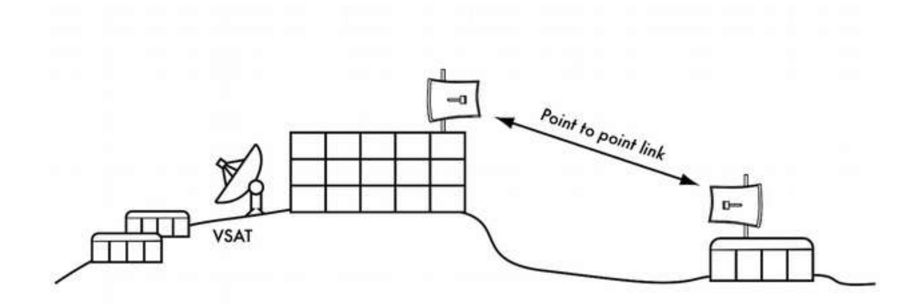


Figura R 17: Un enlace punto a punto le permite a un lugar remoto compartir una conexión central a Internet

Por supuesto, una vez hecha una conexión punto a punto, se pueden añadir otras para seguir extendiendo la red. Si en nuestro ejemplo el edificio alejado se encuentra en la cima de una colina alta, puede ser posible ver otras ubicaciones importantes que no pueden divisarse directamente desde el campus central. Mediante la instalación de otro enlace punto a punto al lugar alejado, se puede unir a la red otro nodo y compartir la conexión central a Internet. Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a Internet. Supongamos que usted debe desplazarse hasta una estación meteorológica alejada, ubicada en lo alto de una colina, para recolectar los datos allí registrados.

Podría conectar el lugar con un enlace punto a punto, logrando la recolección y el monitoreo de datos en tiempo real, sin tener que ir hasta el lugar. Las redes inalámbricas pueden suministrar suficiente ancho de banda como para transmitir grandes cantidades de datos (incluyendo audio y video) entre dos puntos que tengan conexión entre sí, aunque no haya conexión directa a Internet.

Punto a multipunto

El siguiente diseño más comúnmente encontrado es la red punto a multipunto.
Cada vez que tenemos varios nodos hablando con un punto de acceso central estamos en presencia de una aplicación punto a multipunto. El ejemplo típico de un trazado punto a multipunto es el uso de un punto de acceso inalámbrico que le da conexión a varias computadoras portátiles. Las computadoras portátiles no se comunican directamente unas con otras, pero deben estar dentro del alcance del punto de acceso para poder utilizar la red.

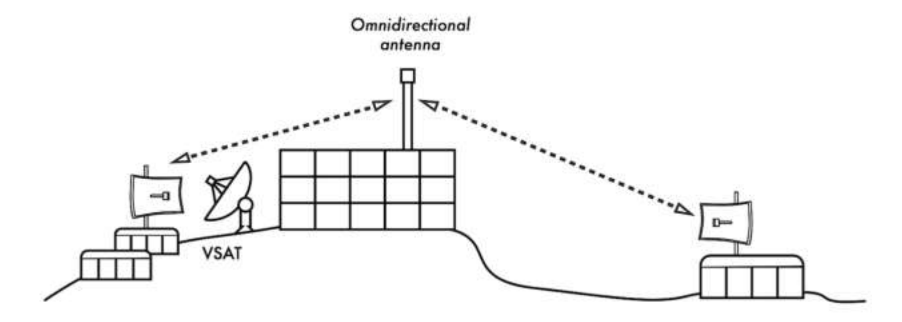


Figura R 18: La conexión VSAT central es ahora compartida por múltiples sitios remotos. Estos tres lugares también pueden comunicarse directamente entre sí a velocidades mucho más rápidas que las ofrecidas por VSAT

La red punto a multipunto también puede ser aplicada a nuestro ejemplo anterior en la universidad. Supongamos que el edificio alejado en la cima de la colina está conectado con el campus central con un enlace punto a punto. En lugar de colocar varios enlaces punto a punto para distribuir la conexión a Internet, se puede utilizar una antena que sea visible desde varios edificios alejados.

Este es un ejemplo clásico de conexión punto (sitio alejado en la colina) a multipunto (muchos edificios abajo en el valle) en áreas extensas.

Hay algunas limitaciones con el uso de enlaces punto a multipunto en distancias muy grandes que van a ser tratadas más adelante en el capítulo **Planificar la Instalación**. Estos enlaces son útiles y posibles en muchas circunstancias, pero no cometamos el clásico error de instalar una torre de radio de gran potencia en el medio de la ciudad esperando darles servicio a miles de clientes, como podría hacerse con una estación de radio FM. Como veremos, las redes de datos de dos vías se comportan de forma muy diferente a las emisoras de radiodifusión.

Multipunto a multipunto

El tercer tipo de diseño de red es el multipunto a multipunto, el cual también es denominado red ad-hoc o en malla (*mesh*). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

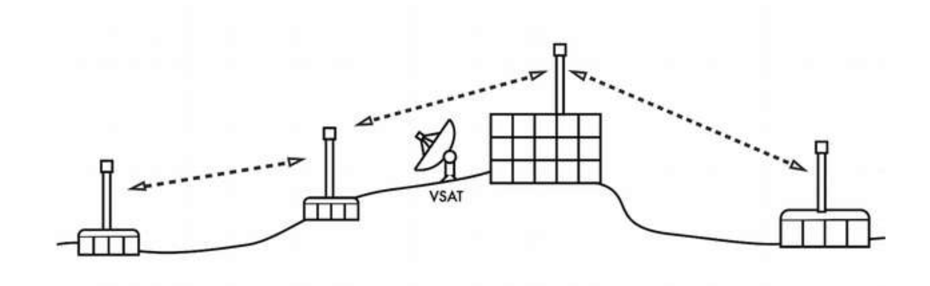


Figura R 19: Una red en malla multipunto a multipunto. Cada punto puede acceder a otro a gran velocidad, o utilizar la conexión central VSAT para acceder a Internet

El beneficio de este diseño de red es que aunque ninguno de los nodos sea alcanzable desde el punto de acceso central, pueden comunicarse entre sí.

Las buenas implementaciones de redes en malla son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen.

Extender una red en malla es tan sencillo como agregar más nodos. Si uno de los nodos en la "nube" es además una pasarela a Internet, esa conexión puede ser compartida por todos los clientes.

Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento. La seguridad de esta red también es un tema importante, ya que todos los participantes pueden potencialmente transportar el tráfico de los demás. La resolución de los problemas de las redes multipunto a multipunto suele ser complicada, debido al gran número de variables que cambian cuando los nodos se conectan y desconectan a Internet. Las redes multipunto a multipunto generalmente no tienen la misma capacidad que las redes punto a punto, o las punto a multipunto, debido a la sobrecarga adicional de administrar el enrutamiento de la red y el uso más intensivo del espectro de radio.

Sin embargo, las redes mesh son útiles en muchas circunstancias. Encontrará más información sobre las redes en malla en el capítulo **Redes en Malla.**

Use la tecnología adecuada

Todos estos diseños de redes pueden ser usados para complementarse unos con otros en una gran red, y también pueden emplear técnicas tradicionales de redes cableadas cuando sea posible. Las redes cableadas todavía tienen más capacidad de ancho de banda que las inalámbricas así que deberían usarse cuando sea apropiado o asequible.

Es una práctica común, por ejemplo, usar un enlace inalámbrico de larga distancia para darle acceso a Internet a un lugar remoto, y luego instalar un punto de acceso en ese sitio para dar acceso local inalámbrico. Uno de los clientes de este punto de acceso puede también actuar como nodo malla (*mesh*), permitiendo que la red se difunda orgánicamente entre usuarios de computadoras portátiles quienes finalmente usarán el enlace punto a punto original para acceder a Internet.

Esto es solamente una posibilidad de utilización de redes inalámbricas, pero hay muchas más.

Ahora que tenemos una idea más clara de la configuración de las redes inalámbricas, podemos comenzar a entender como se realiza la comunicación en dichas redes.

7. LA FAMILIA WIFI

IEEE 802: ¿qué es y por qué es importante?

En los primeros tiempos de las redes existían sólo las redes cableadas (si no se cuentan las viejas líneas del troncal de microondas que cruzaba los Estados Unidos). Hoy en día muchas redes se construyen con soluciones cableadas e inalámbricas. Normalmente las redes basadas en cables, o más comúnmente fibras, tienen más capacidad que las inalámbricas.
Pero instalar fibras es más caro y consume más tiempo. Por esto, a menudo una red comienza como inalámbrica y a medida que crece su utilización se comienzan a instalar fibras. En redes de acceso (las que están cerca del consumidor) o en ambientes urbanos de gran densidad, la solución inalámbrica es también a menudo la más práctica. Así que es importante recordar que si piensa instalar redes inalámbricas en su área o en su comunidad, esa red va a ser la base del crecimiento futuro de las redes en su región. Un aspecto importante sobre las redes cableadas e inalámbricas es la variedad de estándares que existen hoy en día y los nuevos que están desarrollándose. Los estándares inalámbricos son la base de muchos productos inalámbricos, lo que asegura su interoperabilidad y su usabilidad por parte de los que desarrollan, instalan y gestionan redes inalámbricas. Ya hablamos de este tema en el capítulo sobre **Espectro Radioeléctrico.** Los estándares usados en la mayoría de las redes proviene fueron establecidos por los grupos de trabajo 802 del IEEE. IEEE 802 abarca una familia de estándares IEEE para redes locales y de área metropolitana.

Más precisamente, los estándares IEEE 802 son específicos para redes que tratan redes con paquetes de tamaño variable. (A diferencia de las redes en las que los datos se transmiten en pequeñas unidades, de tamaño uniforme llamadas células o celdas). El número 802 simplemente fue el próximo número disponible que le asignó la IEEE, aunque "802" a veces se interpreta como la fecha en que se celebró la primera reunión: febrero de 1980. Los servicios y protocolos especificados en IEEE 802 atañen las dos capas inferiores (Enlace de Datos y Física) del modelo de referencia OSI de siete capas. De hecho, IEEE 802 divide la Capa OSI de Enlace de Datos en dos sub-capas denominadas Control de Enlace Lógico (LLC) y Control de Acceso a Medios (MAC).

La familia de estándares IEEE 802 es mantenida por el Comité de Estándares LAN/MAN de la IEEE (LMSC).
Los estándares más usados son: familia Ethernet, Token Ring, Redes Inalámbricas, Redes Puenteadas y Redes Puenteadas Virtuales.
Cada grupo de trabajo se enfoca en un área específica como aparece en la tabla siguiente.

Nombre	Descripción
IEEE 802.1	Puentes y Gestión de Redes
IEEE 802.3	Ethernet
IEEE 802.11 a/b/g/n	Redes Inalámbricas de Área Local (WLAN)
IEEE 802.15	Redes Inalámbricas de Área Personal (PAN)
IEEE 802.15.1	Bluetooth
IEEE 802.15.2	Coexistencia IEEE 802.15 y IEEE 802.11
IEEE 802.15.3	Redes Inalámbricas de Área Personal (WPAN) y Alta Velocidad
IEEE 802.15.4	Redes Inalámbricas de Área Personal y Baja Velocidad (Por ej. Zigbee)
IEEE 802.15.5	Redes en Malla para WPAN
IEEE 802.15.6	Redes de Área Corporal (BAN)
IEEE 802.16	Acceso Inalámbrico de Banda ancha (base de WiMAX)
IEEE 802.16.1	Servicio de Distribución Local Multipunto (LMDS)
IEEE 802.18	Regulaciones de Radio
IEEE 802.19	Coexistencia
IEEE 802.20	Acceso Inalámbrico Móvil de Banda Ancha
IEEE 802.21	Traspaso (*handoff*) Independiente del Medio
IEEE 802.22	Redes Inalámbricas de Área Regional
IEEE 802.23	Servicios de Emergencia
IEEE 802.24	Malla Inteligente (*Smart Grid*)
IEEE 802.25	Red de Área Omni-Range

El estándar 802.11

El estándar 802.11 es el que más nos interesa ya que define el protocolo para redes Inalámbricas. Las enmiendas a 802.11 son tantas que se ha comenzado desde hace dos años a usar dos letras en lugar de una (802.11z, —la modificación DLS— cedió el paso a 802.11aa, ab, ac..., etc.).

A continuación tenemos una tabla con las variantes de 802.11, sus frecuencias y alcances aproximados.

Proto-colo 802.11	Apro-bado	Fre-cuencia	An-cho de Ban-da	Tasa de datos por flujo	Alcance aproximado en interiores		Alcance aproximado en interiores	
		(GHz)	(MHz)	(Mbit/s)	(m)	(ft)	(m)	(ft)
-	Jun 1997	2.4	20	1, 2	20	66	100	330
a	Sep 1999	5	20	6,9,12, 18, 24, 36, 48, 54	35	115	120	390
b	Sep 1999	2.4	20	1, 2, 5.5, 11	35	115	140	460
g	Jun 2003	2.4	20	6,9,12, 18, 24, 36, 48, 54	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70	230	250	820
			40	15, 30, 45, 60 , 90, 120, 135, 150				
ac	Nov.2011	5	20	Up to 87.6				
			40	Up to 200				
			80	Up to 433.3				
			160	Up to 866.7				

En el 2012, el IEEE publicó el estándar 802.11/2012 que consolida todas las enmiendas previas.
El documento puede descargarse en:

http://standards.ieee.org/findstds/standard/802.11-2012.html

Planificación de instalación de redes inalámbricas 802.11

Antes de que los paquetes puedan ser remitidos y enrutados a la Internet, las capas uno (física) y dos (enlace de datos) tienen que estar conectadas. Sin enlace de conectividad local, los nodos de la red no podrán hablar entre sí ni enrutar paquetes.
Para proporcionar conectividad física, los dispositivos inalámbricos de la red deben operar en la misma zona del espectro radioeléctrico.
Esto significa que los radios 802.11a hablarán con radios 802.11a, a 5 GHz, y los radios 802.11b/g hablarán con otros radios 802.11b/g a 2.4 GHz.
Pero, un dispositivo 802.11a no podrá interactuar con uno 802.11b/g, porque ambos usan partes completamente diferentes del espectro.
Más específicamente, las interfaces inalámbricas deben concordar en un canal común. Si una tarjeta de radio está sintonizada en el canal 2, mientras que otra lo está en el canal 11, los radios no se podrán comunicar. Las frecuencias centrales de cada canal para 802.11a y 802b/g se encuentran en el **Apéndice B: Asignación de Canales.**

Después de que dos interfaces inalámbricas se hayan configurado para usar el mismo protocolo y el mismo canal de radio estarán listas para negociar la conectividad de la capa de enlace de datos. Cada dispositivo 802.11a/b/g puede operar en las siguientes cuatro modalidades.

1. Modo máster (también llamado modo de infraestructura o modo AP) que se utiliza para crear un servicio como el que proporciona un punto de acceso tradicional. La interfaz inalámbrica crea una red con un nombre y un canal específicos (llamado SSID: *Service Set Identifier*) para ofrecer servicios. Cuando están en Modo máster, las interfaces inalámbricas manejan todas las comunicaciones relacionadas con la red (autenticación de clientes inalámbricos, manejo de contención de canales, repetición de paquetes, etc.). Las interfaces inalámbricas en modo máster sólo se pueden comunicar inalámbricamente con interfaces asociadas a ellas en el modo administrado.

2. El modo administrado (*managed*) también se conoce como el modo cliente. Las interfaces inalámbricas en modo administrado se asocian a una red creada por el máster utilizando automáticamente el canal

escogido por este. Luego presentan las credenciales necesarias al máster, y cuando estas son aceptadas, las interfaces están asociadas al máster. Las interfaces en modo administrado no se comunican entre sí directamente sino solamente a través de un máster con el cual están asociadas.

3. El modo ad hoc crea una red multipunto a multipunto donde no hay ningún nodo máster o AP. En modo ad hoc cada interfaz inalámbrica se comunica directamente con sus vecinos. Los nodos deben compartir el mismo nombre y canal y deben poder recibir sus respectivas señales. Los modos ad hoc se conocen a menudo como Redes en Malla y se pueden conseguir más detalles sobre estas en el capítulo **Redes en Malla.**

4. El modo monitor es utilizado por algunas herramientas (como Kismet) para la escucha pasiva del tráfico de radio en un canal determinado. Las interfaces inalámbricas cuando están en modo monitor no transmiten datos. Esto es útil cuando se analizan problemas en un enlace inalámbrico o para la observación del uso del espectro en al área correspondiente. El modo monitor no se usa para las comunicaciones normales.

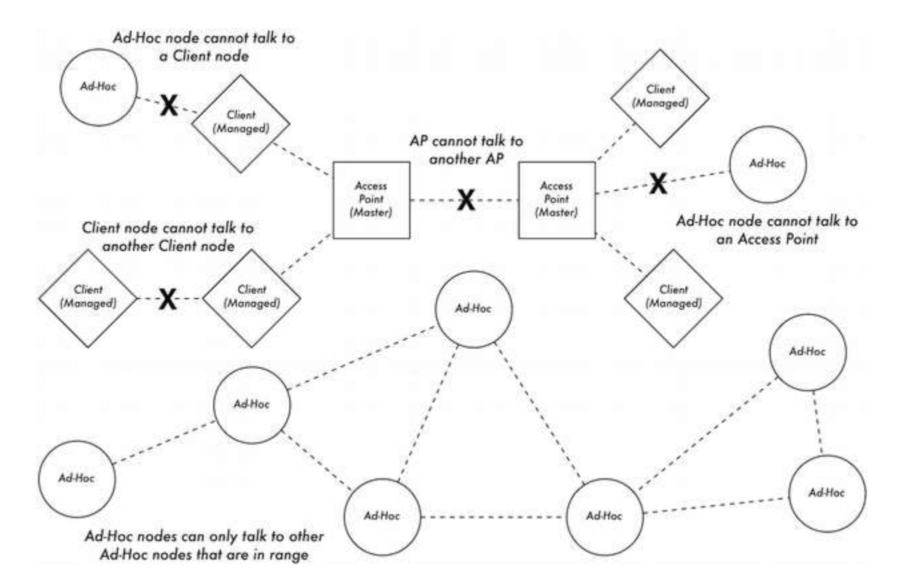


Figura FW 1: Nodos AP, Cliente y Ad hoc

Cuando se implementa un enlace punto-a-punto o punto a multipunto, uno de los radios opera comúnmente en modo máster, mientras que el/los otro(s) operan en modo administrado. En una malla multipunto-a-multipunto, todos los radios operan en modo ad hoc de manera que puedan comunicarse entre sí directamente.
Es importante recordar estos modos cuando se hace el diseño de la red. Recuerde que los clientes en modo administrado no pueden comunicase entre ellos directamente, así que es probable que le convenga configurar repetidor en un sitio elevado en modo máster o ad hoc.
Ad hoc es más flexible pero tiene ciertos problemas de rendimiento, en comparación con el uso de los modos máster/administrado.

El estándar 802.22

¿Se ha preguntado alguna vez por qué uno de los más grandes usuarios del espectro inalámbrico de casi cualquier país del mundo nunca entró en el negocio de la comunicación bidireccional? ¿No? La pregunta sería ¿por qué la Industria de la Comunicación en Televisión no quiso hacer comunicación bidireccional? La respuesta sencilla es que ese no era su interés.
Lo que hicieron en su momento fue buscar el acceso y utilizar 'la flor y nata' del espectro entre la frecuencia 0 y la frecuencia de la luz, que además era casi gratis. Cuando la TV analógica fue reemplazada por la digital, parte de ese espectro privilegiado quedó disponible para redes inalámbricas. Y en algunas partes del mundo donde hay menos instalaciones de TV, estas mismas partes del espectro de radio están disponibles también para redes inalámbricas.
La nueva tecnología inalámbrica es comúnmente denominada TVWS (TV White Spaces) y, si bien es relativamente nueva para el tiempo en que este libro se escribió, ya se está empleando en redes de banda ancha rurales.

Lo que dice Wikipedia:
IEEE 802.22 se conoce informalmente como Súper WiFi, y es un estándar para Redes Inalámbricas Regionales (WRAN) que usa espacios en blanco del espectro de frecuencia de TV.
EL desarrollo del estándar IEEE 802.22 (WRAN) se enfoca en el uso de técnicas de Radio Cognitiva (CR) para permitir el compartir el espectro geográficamente no utilizado asignado al Servicio de Transmisión de Televisión, evitando la interferencia, para permitir el acceso de banda ancha a zonas inaccesibles escasamente pobladas, situación típica en las zonas

rurales; es por lo tanto oportuno y tiene el potencial para una amplia aplicación mundial.

Las WRAN de IEEE 802.22 están diseñadas para operar en las bandas de difusión de TV garantizando que no se producirá interferencia al operador dominante, es decir, para la difusión de TV analógica y digital, y dispositivos licenciados de baja potencia como los micrófonos inalámbricos. El estándar fue publicado finalmente en Julio de 2011.

Tecnología de 802.22 ó TVWS

Las versiones iniciales del estándar 802.22 establecen que la red debería operar en una topología punto a multipunto (p2m). El sistema está formado por una Estación Base (BS) y uno o más Equipos Cliente (CPE) que se comunica inalámbricamente con la BS.

Una característica clave de las BS de las WRAN es que son capaces de detectar el espectro disponible.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) junto con la FCC en los Estados Unidos escogieron un enfoque centralizado para la determinación de espectro disponible. Específicamente, cada Estación Base (BS) estará dotada con un receptor GPS para determinar su posición. Esta información se envía a los servidores centralizados que responderán con la información sobre los canales de TV libre disponibles y las bandas de guardia en el área de la Estación Base.

Otro enfoque está basado solamente en la detección del espectro localmente por parte de la BS para decidir cuáles canales estarían disponibles para la comunicación.

Los CPE analizarán el espectro y enviarán informes periódicos a la BS. Esta, con la información acumulada evaluará si se hace necesario un cambio del canal empleado, o si por el contrario, debe permanecer en el mismo para recibir y transmitir. A esto se llama detección distribuida. Una combinación de ambos enfoques es también concebible.
Estos mecanismos de detección se usan principalmente para identificar si hay alguna transmisión por parte del usuario predominante para evitar interferir con ella. Esto significa que la capa física debe ser capaz de adaptarse a diferentes condiciones y de ser flexible para saltar de canal en canal sin errores de transmisión o pérdida de clientes (CPE).

Esta flexibilidad se requiere también para ajustar dinámicamente el ancho de banda, y los esquemas de modulación codificación. OFDMA *(Orthogonal Frequency-Division Multiple Access)* es el esquema de modulación para transmisión en enlaces ascendente y descendentes. Con OFDMA es posible lograr la rápida adaptación necesaria para la BS y los CPE.

Usando sólo un canal de TV (con un ancho de banda de 6, 7, u 8 MHz, dependiendo del país) la tasa de bits máxima aproximada es de 19Mbit/s a una distancia de 30 km. Conglomerando más de un canal en lo que se conoce como *Channel Bonding* se podrá multiplicar la tasa de transmisión proporcionalmente al número de canales empleados.

Resumen

Como hemos visto, los estándares para instalaciones cableadas e inalámbricas fueron diseñados principalmente en el Grupo de Trabajo de IEEE 802.
Los equipos de la familia de estándares 802.11 son, con mucho, los más fabricados e instalados para enlaces inalámbricos tanto de interiores como de exteriores.
El capítulo **Selección y Configuración del Hardware** habla de equipos en más detalle.

Si se permite el uso del espectro actualmente usado para difusión de TV sin necesidad de licencia, el nuevo estándar 802.22 jugará un papel cada vez más importante en las redes inalámbricas tanto rurales como urbanas.

Al presente, el estándar 802. 22 está todavía en la infancia, y los otros estándares dirigidos a la utilización del espectro de televisión aún no han sido oficialmente aprobados con lo que hay muy pocos equipos disponibles en el mercado para la utilización bidireccional de la frecuencia de TV. Por el momento hay un proyecto interesante en Escocia, Reino Unido, que está utilizando 802.22 en las bandas de televisión.
Información sobre este proyecto:
http://www.wirelesswhitespace.org/projects.aspx

8. REDES EN MALLA

Introducción

Las redes en malla están basadas en instalaciones multipunto a multipunto. En la nomenclatura de la IEEE 802.11, las instalaciones Mp-Mp se denominan redes 'ad hoc' o modo IBSS (*Independent Basic Service Set*).

La mayoría de las redes inalámbricas hoy en día se basan en comunicaciones punto a punto o punto a multipunto.

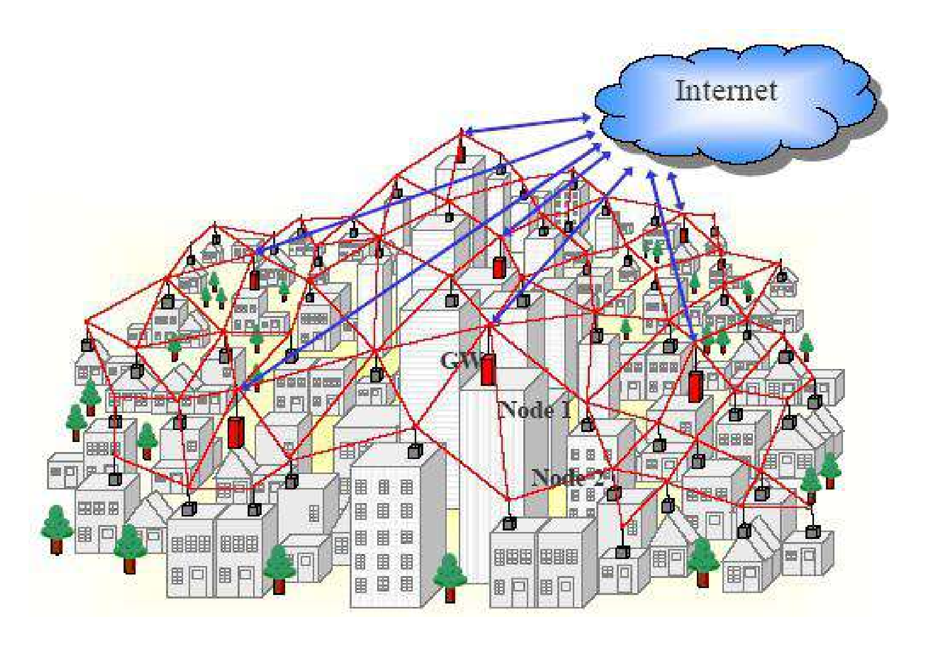


Figura RM 1: Red en malla de área metropolitana que provee conectividad local y acceso a Internet a través de múltiples pasarelas de Internet

Un *hotspot* inalámbrico típico opera en el modo de infraestructura (máster) P-Mp. Consiste en un punto de acceso (access point) con un radio que opera en modo máster conectado a una línea DSL u otra red de otro tipo de largo alcance.

En un *hotspot*, el punto de acceso funciona como una estación máster que distribuye acceso a Internet a sus clientes.
Esta topología centralizada (hub-and-spoke) es también típica del servicio de telefonía celular.
Los teléfonos celulares se conectan a una estación base P-Mp sin la cual no pueden comunicarse entre sí.
Si usted hace una llamada en broma a un amigo que está sentado del otro lado de la mesa, el teléfono envía los datos a la estación base de su proveedor de servicio que puede estar a varios kilómetros de distancia; luego la estación base le reenvía los datos al teléfono de su amigo.
En áreas remotas sin estaciones base, un teléfono GSM es inútil como herramienta de comunicación porque los radios GSM están diseñados de manera tal que no se pueden comunicar directamente entre sí.
Esto contrasta con el caso de los walkie-talkie que pueden comunicarse directamente entre sí siempre y cuando la señal sea suficientemente fuerte.
La radio es por defecto un medio de difusión, y cualquier estación que puede transmitir y recibir podría comunicar Mp-Mp.
Respecto al reto tecnológico, implementar redes Mp-Mp es más exigente que P-Mp o P-P.

Las estrategias para implementar la coordinación del acceso a los canales son más complejas; por ejemplo, no hay una autoridad central para asignación de ranuras de tiempo de transmisión.
Como no hay coordinación central, las estaciones Mp-Mp necesitan ponerse de acuerdo sobre los parámetros de coordinación de las celdas, por ejemplo, la identificación de la celda inalámbrica.

El hecho de que 802.11 le haya dado el nombre "ad-hoc" al modo Mp-Mp de WiFi, sugiere que IEEE concibe las redes Mp-Mp como soluciones espontáneas, provisionales, no óptimas.

La comunicación multipunto a multipunto es, en realidad, más versátil y puede ser más eficiente que la punto a punto, o la punto a multipunto, puesto que estos son casos particulares de la primera.

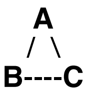
Una red conformada por sólo dos dispositivos multipunto a multipunto, simplemente comunica P-P:

A--B

Una red de tres dispositivos con capacidad de malla A, B, C, pueden conformar una topología como la siguiente:

A--B--C

En esta última, A puede comunicar sólo con B; C puede hacerlo sólo con B, mientras que B puede comunicarse con A y con C. De hecho, B se comunica P-Mp. Pero sin enrutador, A y C no pueden comunicarse directamente en el modo ad-hoc de 802.11.
Al añadir un protocolo de enrutamiento, A puede automáticamente aprender que detrás de B está C y viceversa, y que B puede usarse como un relevo de comunicación de manera que todos los nodos puedan comunicar entre sí. En este caso, B funcionará como un punto de acceso en el modo de infraestructura de 802.11. Las tarjetas WiFi configuradas como clientes en infraestructura no pueden comunicarse directamente, de manera que siempre van a necesitar el punto de acceso B como relevo. Si movemos los tres dispositivos, la topología puede convertirse en una verdadera malla donde cada nodo puede comunicarse con los otros directamente.



En este caso, el relevo del tráfico no es necesario, dado que hay enlaces directos entre todos los nodos. En modo de infraestructura, la comunicación directa no es posible. Todo el tráfico entre los clientes debe ser relevado a través del punto de acceso. Si ahora añadimos D a la topología en cadena del ejemplo, todos los dispositivos pueden comunicarse entre sí, si esto es una malla.

A--B--C--D

Por otra parte, esto no sería posible si la red se hace en modo infraestructura y B es un punto de acceso.

En este caso, C y D serían ambos clientes en infraestructura, y, como ya dijimos, no podrían comunicarse directamente entre sí. El cliente D no podría entrar en la red de infraestructura porque está fuera del alcance del punto de acceso B, aunque esté dentro del alcance del cliente C.

Impacto del ancho de banda en rutas de múltiples saltos

Las redes en malla conformadas por dispositivos que usan un sólo radio son una forma económica para establecer una red inalámbrica ubicua, pero esto tiene una desventaja. Como se tiene una sola interfaz inalámbrica por dispositivo, los radios tienen que operar en el mismo canal. Al enviar los datos desde el nodo A al C a través de B el ancho de banda se reduce a la mitad. Cuando A le envía los datos a B, B y C tienen que quedarse en silencio.

Mientras B le remite los datos a C, A tiene que estar en silencio también, y así sucesivamente. Nótese que esto es lo mismo que pasa cuando dos clientes conectados a un punto de acceso en modo infraestrutura quieren comunicarse entre sí.

Si suponemos que todos los enlaces inalámbricos de la cadena en malla A-B-C-D funcionan a la misma velocidad, la comunicación entre A y D sería más o menos 1/3 de la velocidad de un enlace individual, suponiendo que A y D pueden utilizar la totalidad de la capacidad de la red. Esta reducción del ancho de banda puede evitarse completamente utilizando dispositivos con múltiples radios, dado que estos operarían a diferentes frecuencias que no interfieren entre sí.

A pesar de la desventaja del ancho de banda, los dispositivos en malla con radios únicos tienen su mérito. Son más baratos, menos complejos y consumen menos energía que los dispositivos multi-radio. Esto puede ser importante si el sistema usa energía solar o eólica, o requiere de un respaldo de baterías. Si los enlaces inalámbricos en una red de tres saltos (una cadena con 4 nodos como en el ejemplo) operan a 12Mbit/s cada uno, el ancho de banda total de punta a punta es todavía suficiente para saturar un enlace de 2 Mbit/s a Internet.

Resumen

Las redes en malla extienden el alcance de los dispositivos inalámbricos a través del relevo mutisalto del tráfico. Por medio de un enrutamiento dinámico, las redes pueden auto-restaurarse en caso de que un nodo falle y también crecer orgánicamente cuando se añadan más nodos. Si los nodos de la malla tienen un sólo radio, el beneficio de la cobertura se produce a expensas de la reducción del ancho de banda.

A continuación se presenta un ejemplo de una red en malla instalada. Se puede obtener más información sobre esta instalación en:
http://code.google.com/p/afrimesh/



Figura RM 2: Captura de pantalla de la malla de Villagetelco en Ciudad del Cabo, Sudáfrica

Protocolos de enrutamiento para redes en malla

Los protocolos de enrutamiento para redes inalámbricas en malla tienen que diseñarse teniendo en mente los retos de la comunicación de radio.
Un protocolo de enrutamiento en malla debe ser resistente a los errores de enrutamiento incluso si los mensajes se retrasan o se pierden.
A la vez, el ancho de banda de comunicación disponible y el rendimiento de los nodos malla son limitados, y no deberían malgastarse en decisiones de protocolo y de control de tráfico.
En el 2005, cuando salió la primera edición de este libro, había pocos protocolos de enrutamiento para redes en malla realmente utilizables. En las ediciones previas, el presente capítulo se enfocaba en OLSR.
En ese entonces el 'demonio' OLSR no venía en la configuración por defecto, así que era necesario navegar en las profundidades del archivo olsrd.con para averiguar cuál era la mejor configuración del algoritmo de enrutamiento.

La situación ha cambiado un poco desde el 2005.
En este momento hay un buen número de protocolos de malla e implementaciones; todas las implementaciones mencionadas en este capítulo están disponibles como paquetes de instalación para OpenWRT.
Los creadores de protocolos para malla compiten en un desafío para producir los mejores protocolos. Hay incluso una competencia para estos creadores que se celebra una vez al año y que se llama 'Battlemesh', www.battlemesh.org
La mayor parte de los protocolos de enrutamiento en malla (BABEL, BATMAN, OLSR, BMX, BMX6) se preocupan por mantener las tablas de enrutamiento Ipv4 e Ipv6 en un nodo de la malla usando el procedimiento de añadir, actualizar y borrar rutas. Estos protocolos usan enrutamiento basado en IP. Son protocolos de capa 3, puesto que IP representa la tercera capa del modelo OSI para redes.
Batman-adv(anced) es un protocolo relativamente nuevo que opera en la segunda capa del modelo de instalación de redes, por lo tanto es un protocolo de malla de capa 2. En las capas superiores (incluida IP), Batman-adv hace que la malla completa parezca un interruptor, donde todas las conexiones son de enlace local (link-local). Una malla Batman-adv es transparente para las capas superiores del modelo de redes.
Esto simplifica bastante la instalación de una red en malla porque es posible usar DHCP, mDNS o puente MAC con Batman-adv. Batman-adv es un módulo kernel de Linux que viene con las fuentes kernel oficiales de Linux.
Los protocolos de enrutamiento para mallas deberían gestionar también el anuncio y selección de pasarelas a redes externas como Internet.
Un problema común con los mecanismos de selección de pasarelas es que el protocolo de enrutamiento podría decidir cambiar de pasarelas con mucha frecuencia, por ejemplo, cuando una vía de enrutamiento hacia una pasarela haya mejorado ligeramente con respecto a otra. Esto es un problema porque puede ocasionar inestabilidad en el acceso a Internet.
Si hay más de una pasarela a Internet en la malla, es muy recomendable emplear un método avanzado de selección de pasarelas.

¿Y qué hay sobre los estándares 802.11s?

La meta de 802.11s es de servir hasta 32 nodos. Según Wikipedia, utiliza protocolos HWMP (Hybrid wireless mesh protocol), es decir, usa protocolos de malla híbridos e inalámbricos como los protocolos de enrutamiento por defecto, con la opción de usar otros protocolos de enrutamiento.

Citando: “HWMP se inspira en una combinación de AODV (RFC 3561 [2]) y el enrutamiento basado en árbol (tree-based)”. Puesto que 802.11s es relativamente nuevo, hasta ahora no hay mucha experiencia práctica.

Dispositivos y firmware para los dispositivos integrados

No todos los dispositivos WiFi del mercado son apropiados para instalar redes en malla. En el 2005, cuando salió a la luz la primera edición de este libro, una de las recomendaciones claras como hardware para redes en malla era el enrutador Linksys WRT54G en combinación con el firmware Freifunk. Aunque el WRT54G(L) está todavía en el mercado, ya no se recomienda.[1] El OpenWRT es un ambiente para desarrollo de firmware muy versátil y a la vez un firmware para usuarios avanzados de Linux.

El clásico firmware Freifunk se basa en la versión desactualizada de OpenWRT 'White Russian'. Esta versión “White Russian” respaldaba sólo dispositivos con chipsets Broadcom, con un driver binario inalámbrico privativo, basado en Linux 2.4. Ha sido superado por las versiones OpenWRT 'Kamikaze' y 'Backfire' (más nuevo). Con 'Kamikaze' y 'Backfire', OpenWRT ofrece soporte para diferentes chipsets inalámbricos, dispositivos y arquitecturas de CPU.

La próxima versión estable de OpenWRT se llamará 'Attitude Adjustment', la cual, al momento de esta versión del libro está en la fase de 'candidato a salir'. Los puertos de plataforma 'AR7xxx' y 'Atheros' de la versión 'Attitude Adjustment' se consideran estables.

Todos los protocolos de enrutamiento para redes en malla mencionados se encuentran disponibles como paquetes de instalación para OpenWRT. Sólo unas pocas comunidades de redes abiertas han desarrollado sus propias imágenes personalizadas de firmware usando OpenWRT Kamikaze y Backfire.

Sin embargo, lo han hecho para satisfacer referencias y requisitos locales. Por esta razón podría no ser práctico para el uso público general. OpenWRT tiene un sistema de gestión de paquetes que viene

1. Aunque el WRT54G(L) se encuentra en el mercado todavía, el precio de 60 US$ es excesivo. La revisión 4.0 de WRT54G fue vendida por Linksys como revisión WRT54G 1.0 en el 2005, después de que Linksys ya había introducido la revisión WRT54G 5.0 que ya no era compatible con Linux. La revisión WRT54G 5.0 tiene solamente la mitad del almacenamiento flash y de capacidad RAM. El modelo WRT54G 5.0 es el enrutador WiFi que ha estado en producción más tiempo. Con el dinero que se necesitaba gastar en 2011 para comprarse un Linksys WRT54G 5.0, se podían comprar dos o tres dispositivos semejantes de otras marcas, y más veloces en términos de CPU y tasa de datos.

al rescate. Es típico de OpenWRT instalar paquetes de programas en el enrutador después de la instalación inicial. En estos momentos hay un meta-paquete llamado 'luci-freifunk-community' que convierte automáticamente una imagen OpenWRT en un firmware de redes en malla.
El número de dispositivos que pueden convertirse en un enrutador en malla ha aumentado notablemente. Por otra parte, el proceso de convertir un firmware OpenWRT en un firmware para malla a través del sistema de manejo de paquetes es, desafortunadamente, cada vez más susceptible de errores. Algunos fabricantes de enrutadores WiFi entregan dispositivos que vienen con OpenWRT como su firmware de fábrica, por ejemplo Mesh-Potato, Dragino MS-12, Alnet 0305.



Figura RM 3: Mesh-Potato, un enrutador WiFi de exteriores con VoIP (con un puerto FXS para conectar un teléfono analógico www.villagetelco.org

El Mesh-Potato es un dispositivo para uso de exteriores de bajo consumo diseñado para redes en malla con un puerto FXS (teléfono analógico) de manera que se le puede conectar un aparato telefónico y hacer llamadas por la red de malla.
El Mesh-Potato se entrega con un firmware de malla que usa el protocolo de malla Capa 3 BATMAN.

Hay un segundo firmware llamado SECN (Small enterprise/campus network) disponible para el Mesh-Potato, que usa protocolo de malla BATMAN-ADV Capa 2.
De nuevo, la selección de dispositivos disponibles es tan diversa que no hay un método único actualizado que podamos describir que funcione para toda la gama de hardware.

La tabla de hardware que funciona con OpenWRT es inmensa y sigue creciendo:
http://wiki.openwrt.org/toh/start

Este debería ser el primer sitio a revisar antes de salir a comprar cualquier dispositivo.

Por el momento, si está buscando un enrutador basado en un chipset compatible con 802.11 en modo ad hoc, mi recomendación son los dispositivos compatibles con el puerto AR7XXX del OpenWRT.

Note que los fabricantes de hardware pueden cambiar los chipsets de los dispositivos sin hacer mención explícita. No se garantiza que las nuevas versiones de hardware funcionen a menos que alguien las haya probado y reportado en la wiki de OpenWRT.

Algunos dispositivos compatibles con OpenWRT son las unidades para exteriores de Ubiquiti y los dispositivos SOHO (Small Office Home Office) de TP-Link.
TP- Link produce varios dispositivos SOHO de bajo costo con chipsets Atheros ar71xx (802.11n).
El TP-Link MR3220 (802.11n de un sólo flujo) y el MR3420 (802.11n doble flujo) constan de un CPU Mips 24 kc de 400 MHz, un puerto USB 2.0, un conmutador de 4 puertos de 100 Mbit/s, un puerto WAN, 4MB de flash y 32MB de RAM.
Los precios van desde 30US$ en adelante.

Puesto que los dispositivos TP-Link tienen un puerto USB 2.0 es factible añadir otra interfaz WiFi a través de un dongle WiFi. De hecho, USB 2.0 permite muchas posibilidades, como añadir espacio de almacenamiento adicional, soporte de audio, webcams, etc.



Figura RM 4: Enrutadores de bricolaje (DIY) para exteriores construidos a partid de dispositivos SOHO comerciales (la foto muestra ejemplos basados en TP-Link WR741 y WR941, y en un enrutador Fonera

Otra distribución de firmware que inicialmente se originó como alternativa del WRT54G es el DD-WRT que es una distribución de firmware diseñada para usuarios finales. Sólo soporta el protocolo de enrutamiento OLSR.

Problemas frecuentes

Los problemas típicos de la comunicación multipunto a multipunto se encuentran bien sea en la capa física o en la capa MAC. Las sugerencias presentadas por el 802.11 del IEEE sobre los mismos, no son satisfactorias. Los retos principales son:

Coordinación del acceso al canal, es decir, el problema del nodo escondido y el nodo expuesto.

Volviendo a nuestra pequeña red en malla con la topología A B C, puede suceder que A y C empiecen a mandarle datos a B al mismo tiempo porque ellos no se ven entre sí, lo que resulta en una colisión en B. 802.11 tiene un mecanismo para subsanar esta situación: RTS/CTS (solicitud para enviar/libre para enviar: *request to send, clear to send*)

Supongamos que A quiere comunicarse con C que no está dentro de su alcance, por lo tanto envía un paquete RTS que será recibido sólo por B, que replicará con un paquete CTS el cual es escuchado tanto por A como por C y por lo tanto C dejará el canal libre a la transmisión de A.

Sin embargo, el funcionamiento actual RTS/CTS trabaja bien sólo en rutas de 2 saltos. En rutas más largas puede ocurrir que múltiples estaciones envíen señales RTS lo cual resultaría en que todos los nodos detengan sus transmisiones esperando una señal CTS. A esto se le denomina tormenta de transmisión RTS. Para redes en malla de tamaño considerable, el mecanismo RTS/CTS no es recomendable.

Sincronización del reloj

La gente que diseñó el protocolo ad hoc de 802.11 pensó que sería inteligente si los dispositivos WiFi pudieran sincronizar sus relojes MAC por medio del envío de marcas de tiempo en baliza (beacon).
Sin embargo, pueden presentarse marcas de tiempo falsas por defectos del programas y a veces se producen discrepancias (race conditions) debido a diferencias en los tiempos de propagación en el hardware, y en los controladores. Los intentos fallidos para sincronizar las marcas de tiempo a veces se traducen en división de celdas (ver abajo).
Hay algunas estratagemas que se han integrado para solventar este problema.
La mejor solución es deshabilitar completamente la sincronización del reloj. Sin embargo, esta sincronización a veces se hace en el hardware o software de la interfaz inalámbrica.

El OpenWRT permite deshabilitar la sincronización del reloj

cuando se usan tarjetas Atheros 802.11abg que trabajan con el controlador Madwifi. Si está usando un kernel Linux reciente, algunos drivers inalámbricos (como ath9k) que se usan a menudo para dispositivos de malla son bastante robustos respecto a los problemas de reloj en el modo ad-hoc.
Sin embargo, esto no ayuda si el dispositivo WiFi viene con un firmware binario de fuente cerrada que no está diseñado para resolver de manera elegante problemas de reloj. No hay mucho qué hacer al respecto sino utilizar drivers/firmware/chipsets con una confiabilidad demostrada.

División del IBSS en celdas

Este es un problema típico consecuencia de la sugerencia de 802.11 para la implementación del modo Mp-Mp.

Si los dispositivos ad hoc no logran ponerse de acuerdo en utilizar un determinado identificador de celda (cell-id; IBSS-ID) se constituirán celdas inalámbricas separadas desde el punto de vista lógico.

Y el asunto llegaría hasta aquí porque los dispositivos inalámbricos no serán capaces de comunicarse entre sí. El problema se relaciona con la sincronización del reloj. A partir de Linux 2.6.31 es posible fijar manualmente la IBSS-ID. Esta característica también la encontramos en OpenWRT.

9. SEGURIDAD PARA REDES INALÁMBRICAS

Introducción

Aunque que el espectro sin licencia le proporciona un gran ahorro al usuario, tiene el efecto secundario de que los ataques de Denegación de Servicio (DoS: Denial of Service) se producen con sorprendente facilidad. Con sólo encender un punto de acceso de alta potencia, un teléfono inalámbrico, un transmisor de video u otro dispositivo de 2.4 GHz, una persona malintencionada puede causarle un daño considerable a la red. Muchos dispositivos de red son también vulnerables a los ataques de denegación de servicio, como inundación de disociaciones (disassociation flooding) y desborde de las tablas ARP. Hay varias categorías de individuos que pueden causar problemas a una red inalámbrica:

Usuarios no intencionales

Las áreas muy pobladas como los centros de las ciudades o los campus universitarios pueden generar una densidad de puntos de acceso inalámbricos. En estos ejemplos, es común que los usuarios de portátiles se asocien accidentalmente a la red equivocada.
La mayoría de los clientes inalámbricos simplemente elegirán la red inalámbrica que esté disponible, escogiendo a menudo, la que tenga la señal más fuerte cuando la red preferida no está disponible.
El usuario puede en este caso usar esta red como lo hace normalmente, sin saber que puede estar transmitiendo datos confidenciales en la red de otra persona.
Las personas malintencionadas pueden aprovecharse de esta situación colocando puntos de acceso en lugares estratégicos para atraer personas desprevenidas y captar sus datos. El primer paso para evitar este problema es educar a los usuarios subrayando la importancia de conectarse sólo a redes conocidas y confiables.
Muchos clientes inalámbricos pueden configurarse de manera que se conecten solamente a redes confiables o para que pidan permiso antes de incorporarse a una red nueva.
Como veremos más adelante en este capítulo, los usuarios pueden conectarse a redes públicas utilizando encriptación fuerte.

War drivers

El fenómeno de los *war drivers* o buscadores de redes basa su nombre en la famosa película del 1983 sobre piratas informáticos titulada Juegos de Guerra (*War Games*).

Los buscadores de redes están interesados en encontrar la ubicación física de las redes inalámbricas. En general, se mueven por la ciudad equipados con una portátil, un GPS, y una antena omnidireccional, registrando el nombre y la ubicación de cada red que localizan. Luego, combinan estos registros con los de otros buscadores de redes y los transforman en mapas gráficos que describen las "huellas" inalámbricas de la ciudad en cuestión.

La gran mayoría de los buscadores de redes no representa una amenaza directa a la red, pero los datos que recolectan pueden ser de interés para aquellos que se dedican a atacar redes.

Por ejemplo, un punto de acceso desprotegido, detectado de esta manera, podría estar ubicado en un edificio importante, como una oficina de gobierno o una empresa. Una persona malintencionada podría usar esta información para acceder a esa red ilegalmente.

La instalación de ese AP nunca debió haberse hecho, en primer lugar, pero los buscadores de redes hacen más urgente la solución de este problema.

Como veremos más adelante en este capítulo, los buscadores de redes que utilizan el famoso programa NetStumbler pueden ser detectados con otros programas como Kismet. Para más información sobre los buscadores de redes, consulte los sitios:

http://wigle.net/,
http://www.nodedb.com/, or http://www.stumbler.net/.

Puntos de acceso piratas

Hay dos clases de puntos de acceso piratas:

Los instalados incorrectamente por usuarios legítimos, y los instalados por malintencionados que planean recolectar datos o dañar la red.

En el caso más sencillo, un usuario legal de la red podría querer una mejor cobertura inalámbrica en su oficina, o puede ser que encuentre muy difícil cumplir con las restricciones de seguridad de la red inalámbrica corporativa. En este caso, si instala sin autorización un punto de acceso de bajo costo para usuarios, va a abrir la red a ataques potenciales desde el interior. Si bien existe la posibilidad de rastrear a través de la red cableada los puntos de acceso no autorizados, es muy importante establecer desde el comienzo políticas claras que los prohiban.

Puede que sea muy difícil lidiar con la segunda clase de puntos de acceso piratas. Al instalar un AP de gran potencia que utilice el mismo ESSID de la red, una persona malintencionada puede engañar a la gente para que usen su equipo y de esta manera registrar o manipular todos los datos que pasen a través de él. Repetimos: si sus usuarios están entrenados para usar encriptación fuerte, este problema se va a reducir de manera significativa.

Escuchas subrepticias

Como mencionamos antes, este es un problema muy difícil de manejar en las redes inalámbricas. Utilizando una herramienta de monitoreo pasiva (como Kismet), un fisgón puede registrar todos los datos de la red desde lejos sin que ni siquiera se note su presencia. Los datos que estén encriptados simplemente pueden registrarse y descifrarse más tarde, mientras que los datos sin encriptación se pueden leer fácilmente en tiempo real. Si a usted le es difícil convencer a otros de este problema, puede realizar una demostración con herramientas como Driftnet.
(http://www.ex-parrot.com/~chris/driftnet/).
Driftnet busca datos gráficos en redes inalámbricas, tales como archivos GIF y JPEG. Mientras que los usuarios están navegando en Internet, esta herramienta despliega en un collage todos los gráficos encontrados. Usted le puede decir a un usuario que su correo electrónico es vulnerable si no tiene encriptación, pero nada le hace llegar mejor el mensaje que mostrarle las fotos que él/ella está mirando en ese momento en el navegador web. Pero repetimos, las escuchas subrepticias no pueden prevenirse por completo, aunque el uso de una encriptación fuerte apropiada sí va a desalentarlas.

Protección de la red inalámbrica

En una red cableada tradicional, el control del acceso es muy sencillo: si una persona tiene acceso físico a una computadora o a un concentrador (*hub)* en la red, entonces puede usar (o abusar) de los recursos de la red. Si bien los mecanismos de software son un componente importante de la seguridad de la red, el mecanismo decisivo es limitar el acceso físico a los dispositivos de la red.

En pocas palabras: si sólo las personas de confianza tienen acceso a los terminales y los componentes de la red, entonces la red puede considerarse confiable.

Las reglas cambian significativamente en las redes inalámbricas. A pesar de

que el alcance aparente de su punto de acceso puede ser de un centenar de metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso de su red aunque esté a varias manzanas de distancia. Aún cuando un usuario no autorizado sea detectado, es imposible "rastrear el cable" hasta el lugar donde está esa persona. Sin transmitir ni un sólo paquete, un usuario malintencionado experto puede registrar todos los datos de la red inalámbrica en el disco. Más adelante, estos datos pueden utilizarse para lanzar un ataque más sofisticado contra la red. Nunca suponga que las ondas de radio simplemente "se detienen" en el límite de su propiedad o de su edificio. La seguridad física de las redes inalámbricas se limita a prevenir los daños de los componentes activos, los cables y la fuente de alimentación.

Donde el acceso físico a la red no puede ser evitado, tenemos que apoyarnos en los medios electrónicos para el control de la infraestructura inalámbrica de manera que solamente las personas y sistemas autorizados usen la red inalámbrica. Recuerde que a pesar de que una cierta dosis de control al acceso y autenticación es necesaria en cualquier red, usted fracasará en su trabajo si los usuarios legítimos encuentran dificultades para acceder a ella. Por último, aún en las redes cableadas es casi imposible confiar por completo en todos los usuarios de la red. Un empleado descontento, un usuario con poca capacitación, así como una simple equivocación de un usuario honesto pueden causar daño significativo en las operaciones de la red.

Como arquitecto de la red, su objetivo debe ser facilitar la comunicación privada entre los usuarios legítimos de la misma y entre usuarios legítimos y servicios. Según un viejo dicho, la única forma de mantener completamente segura una computadora es desenchufarla, ponerla dentro de una caja fuerte, destruir la llave y enterrar todo bajo concreto. Si bien este método puede ser completamente "seguro", no es útil para la comunicación. Cuando tome decisiones de seguridad para su red, recuerde que por encima de todo, la red existe para que los usuarios puedan comunicarse. Las consideraciones de seguridad son importantes, pero no deben interponerse en el camino de los usuarios. Una simple pista sobre si la red les está planteando problemas a los usuarios es observar la cantidad de tiempo que usted u otro colega estén empleando en ayudarlos a incorporarse a la red.
Si un usuario normal constantemente tiene dificultades para acceder a la red aún después de recibir instrucciones y entrenamiento para hacerlo, es posible que los procedimientos de acceso sean complicados y entonces se impone revisarlos.

Tomando todo esto en cuenta, nuestro objetivo es el de proporcionar una seguridad física adecuada, controlar el acceso y proteger la comunicación sin sacrificar la facilidad del uso.

Seguridad física para redes inalámbricas

Cuando instala una red, usted está construyendo una infraestructura de la cual la gente dependerá. Las medidas de seguridad existen para garantizar que la red sea confiable. Las redes tienen componentes físicos como cables y cajas, cosas que pueden ser dañadas fácilmente. En muchas instalaciones, puede ser que la gente no sepa qué tipo de equipamiento se ha instalado, o experimenten por pura curiosidad. Puede que no se den cuenta de la importancia de un cable conectado a un puerto. Es posible que alguien mueva un cable Ethernet para conectar su computadora portátil durante 5 minutos, o cambie de posición el conmutador porque les estorba. Un enchufe puede ser desconectado de una toma de corriente porque alguien más necesita esa conexión. Garantizar la seguridad física de la instalación es un asunto prioritario. Los letreros y las etiquetas les serán útiles sólo a aquellos que saben leer, o que hablan su mismo idioma. Colocar el equipo donde no estorbe y limitar el acceso al mismo es el mejor medio para asegurarse de que no ocurran accidentes o se manipule el equipamiento. En su localidad puede que no sea fácil encontrar los sujetadores, amarres o cajas apropiados. Sin embargo, es probable que encuentre productos eléctricos equivalentes que funcionen igualmente bien. La fabricación local de cajas para alojar el equipo puede se económicamente viable y debe considerarse esencial para cualquier instalación. A menudo es más económico pagar a un albañil para que haga las perforaciones e instale los conductos. Se puede incrustar una tubería de PVC en las paredes de bloque para pasar el cable de una habitación a otra, evitando así hacer perforaciones cada vez que tenemos que pasar un cable. Para el aislamiento, se pueden rellenar los conductos alrededor del cable con bolsas de plástico. El equipo pequeño debe montarse en la pared y el grande se debe colocar en un armario o gabinete.

Conmutadores

Los conmutadores, concentradores (*hubs)*, o los puntos de acceso interiores pueden atornillarse directamente a la pared. Lo mejor es poner el equipo lo más alto posible para reducir las posibilidades de que alguien toque los dispositivos o sus cables.

Cables

De ser posible, los cables deberían estar ocultos y atados. Es posible encontrar conductos de plástico para cables que pueden usarse en edificios. Si no los encuentra, sujete los cables a la pared para que queden fijos, y asegúrese de que no queden expuestos en lugares donde puedan ser enganchados, pinchados o cortados. Cuando fije los cables en la pared, asegúrese de no clavar o atornillar encima del mismo. El cable está formado de pequeños hilos por donde viajan los datos de la red.

Si perfora el cable con un clavo, lo daña y lo inutiliza para la transmisión de datos. También asegúrese de no torcerlo, o doblarlo en exceso, porque esto también lo daña.
Es preferible enterrar los cables, en lugar de dejarlos colgando en espacios donde puedan ser usados para colgar ropa o ser tropezados con una escalera, etc. Para evitar alimañas e insectos use ductos eléctricos plásticos. El costo adicional vale la pena pues evitará molestias. El ducto debería enterrarse aproximadamente a 30 cm de profundidad, o por debajo del nivel de congelamiento en climas fríos. Es aconsejable comprar ductos de un calibre superior al mínimo necesario de manera que en el futuro se puedan pasar otros cables por el mismo conducto. Considere señalizar los cables enterrados con un aviso de "llame por teléfono antes de excavar" para evitar apagones accidentales.

Energía

Lo mejor es poner los multienchufes (regletas, zapatillas) dentro de un armario cerrado. Si esto no es posible colóquelos debajo de un escritorio, o en la pared y utilice cinta adhesiva fuerte para asegurar el enchufe a la conexión de la pared. No deje espacios libres en el multienchufes ni en la UPS, tápelos con cinta si es necesario. La gente va a tender a utilizar la conexión que esté más a su alcance, por lo tanto hágalas difíciles de usar. Si no lo hace, puede encontrarse con un ventilador o una lámpara enchufada en su UPS; aunque es bueno tener luz ¡es aún más importante mantener su servidor en funcionamiento!

Agua

Proteja su equipo del agua y de la humedad. En todos los casos asegúrese de que su equipo, incluida su UPS, está al menos a 30 cm del piso para evitar daños por posibles inundaciones.

También intente tener una cubierta sobre su equipo, para evitar que le caiga agua y humedad. En climas húmedos es importante que el equipo tenga la ventilación adecuada para asegurarse de que la humedad se disipe. Los armarios pequeños deben tener ventilación, o de lo contrario la humedad y el calor pueden degradar o aún destruir su equipo.

Mástiles

El equipo instalado en un mástil o torre, a menudo está a salvo de los ladrones. No obstante, para disuadirlos y mantener su equipo a salvo del viento es bueno sobredimensionar estos montajes. Los equipos que se monten sobre la torre o mástil deben pintarse de colores apagados, blanco o gris mate para reflejar el sol, y para desviar la atención, haciéndolo lucir poco interesante. Las antenas tipo panel son más imperceptibles y atractivas que los reflectores parabólicos y por eso debemos preferirlas. Todas las instalaciones en las paredes deberán estar a una altura tal que se requiera de una escalera para alcanzarlas. Elija lugares bien iluminados pero no muy destacados para poner el equipo. También evite las antenas que se parezcan a las de televisión, porque esas pueden atraer el interés de los ladrones, mientras que una antena WiFi no va a ser de utilidad para la mayoría de ellos.

Autenticación y control de acceso

Cuando se habla de autenticación, surgen un número de términos relacionados, tales como identidad (digital), autorización, privacidad, etc. Así que antes de entrar en el tema de la autenticación *per se*, vamos a presentar la terminología sin intención de ser exhaustivos.

La identidad digital es la entidad electrónica que representa a una entidad física, como una persona o un dispositivo. La autenticación es el proceso de verificar la afirmación de que una cierta entidad (electrónica) tiene permiso para actuar en representación de una determinada entidad (física). En otras palabras, la autenticación es el proceso de comprobación de que una entidad física se corresponde con una entidad electrónica.

La autorización, en cambio, es el proceso de establecer los derechos de una identidad para acceder a determinados recursos o para ejecutar ciertas acciones.

Por último, la privacidad es un asunto complejo, pero tiene que ver con los derechos que tiene una persona de que sus datos o conducta privada no sean conocidos por gente que, estrictamente hablando, no los necesita para proporcionar el servicio solicitado. Por ejemplo, es razonable que una licorería quiera saber que un cliente es mayor de edad antes de venderle alcohol, pero lo no es que se averigüe su nombre y mucho menos que los datos de la transacción se transmitan a otra gente.

La privacidad es una preocupación especial en un mundo en el que los usuarios hacen uso cada vez más frecuente de las redes y servicios fuera de sus casas. Sin una debida atención a los aspectos de privacidad, es muy fácil rastrear la conducta y los movimientos de los usuarios.

Es digno de mención que existe un compromiso entre la autenticación y la privacidad. El hecho de verificar la identidad de un usuario ya constituye una invasión a su privacidad, el ente autenticador sabe quién está usando un cierto recurso, a qué hora y dónde, pero el reto es minimizar la cantidad de información sobre el usuario y del número de personas que tiene acceso a esa información.

En el contexto de este libro estamos principalmente interesados en las técnicas de control de acceso a la red. En pocas palabras, queremos ser capaces de decidir quién (de identidad autenticada) tiene acceso a qué cosa (autorización) sin sacrificar la privacidad.

La autenticación se realiza normalmente por medio de la prueba del conocimiento de un secreto (una contraseña, una firma), o de la posesión de una señal o característica (un certificado, una huella dactilar), o ambos. El control de acceso es a menudo necesario para asegurarse de que sólo los usuarios autorizados puedan usar la red, con la finalidad de prevenir el agotamiento de los limitados recursos y/o para dar cumplimiento a normas reguladoras. Además de redes con control de acceso, puede haber redes abiertas con acceso limitado o con tiempo limitado, pero debido a la necesidad de las organizaciones de controlar el acceso a recursos limitados, o por la existencia de leyes anti-terrorismo, estas redes son menos comunes. Durante años se han empleado un número de técnicas para el control de las redes inalámbricas. Posteriormente se han ido abandonando, por problemas de seguridad o de escalabilidad a medida que la WiFi se hace más popular.

Filtrado de MAC

El acceso a la red WiFi puede estar restringido por la dirección MAC. Esta consiste en un número de 48 bits asignado por el fabricante de cada dispositivo inalámbrico o Ethernet y se supone que es único y permanente.

Si usamos filtrado MAC en nuestros puntos de acceso, podemos autenticar a los usuarios con base en sus direcciones MAC. Con esta modalidad, el punto de acceso mantiene una tabla interna de direcciones MAC aprobadas. Cuando un usuario intenta asociarse a un punto de acceso, la dirección MAC del cliente debe estar en la lista aprobada, o de lo contrario la asociación va a ser rechazada. Como una alternativa, el AP puede tener una tabla de direcciones MAC "prohibidas", y habilitar a todos los dispositivos que no estén en esa lista.

Desafortunadamente, este no es un mecanismo de seguridad ideal. Mantener las tablas MAC en cada dispositivo puede ser muy engorroso, y requiere que todos los dispositivos cliente tengan su dirección MAC grabadas y cargadas en los AP. Además, las direcciones MAC a menudo pueden modificarse mediante software. Si un atacante determinado observa las direcciones MAC que están en uso en una red inalámbrica, él puede "suplantar" una dirección MAC aprobada y asociarse con éxito al AP.

A pesar de que el filtro MAC va a evitar que los usuarios involuntarios y los curiosos accedan a la red, el filtro MAC por sí sólo no puede proteger su red de los atacantes empecinados. Los filtros MAC son útiles para limitar temporalmente el acceso de usuarios que actúan de forma incorrecta. Por ejemplo, si una computadora portátil tiene un virus que envía grandes cantidades de spam u otro tráfico no deseado, su dirección MAC puede agregarse a la tabla de filtrado para detener el tráfico de forma inmediata. Esto nos dará tiempo para ubicar al usuario y arreglar el problema.

Redes cerradas

Otra forma que fue popular como "modalidad de autenticación" de las redes inalámbricas fue la de *red cerrada*. En una red común, los AP transmiten sus ESSID muchas veces por segundo, permitiéndoles a los clientes inalámbricos (así como a las herramientas del tipo NetStumbler) encontrar la red y mostrar su presencia al usuario. En una red cerrada, el AP no transmite el ESSID (ESSID oculto), y los usuarios deben conocer el nombre completo de la red antes de que el AP les permita asociarse. Esto evita que los usuarios casuales descubran la red y la seleccionen en su cliente de red inalámbrica.

Con este mecanismo hay varios inconvenientes. Forzar a los usuarios a escribir el ESSID completo antes de conectarse a la red, amplía las posibilidades de error y a menudo resulta en solicitudes de soporte y quejas.

Ya que la red no se hace manifiestamente presente para los dispositivos de rastreo de sitios, como NetStumbler, esto puede prevenir que la misma aparezca en los mapas de los *war drivers*. Pero también significa que otros instaladores de redes tampoco pueden encontrar su red con facilidad, y no van a saber que usted está usando un canal dado. Un vecino podría realizar un estudio del lugar, y al no detectar redes cercanas podría instalar su propia red en el mismo canal que usted está utilizando, lo cual va a provocarle problemas de interferencia tanto a usted como a su vecino.

Finalmente, utilizar redes cerradas ofrece poca seguridad adicional a su red. Utilizando herramientas de monitoreo pasivas (como Kismet), un usuario malintencionado puede detectar paquetes enviados desde sus clientes legítimos al AP. Esos paquetes necesariamente contienen el nombre de la red. Y por lo tanto, el malintencionado puede usarlo luego para asociarse, al igual que lo haría un usuario normal.

Probablemente la encriptación sea la mejor herramienta que tenemos para autenticar a los usuarios de la red. Mediante una encriptación fuerte, podemos identificar a un usuario de una forma única difícil de suplantar, y usar esa identidad para determinar accesos futuros a la red. La encriptación también tiene el beneficio de ofrecer una capa adicional de privacidad ya que evita que los fisgones tengan un acceso fácil al tráfico de la red.

La encriptación es la técnica utilizada para la autenticación de usuarios en la mayoría de las instalaciones actuales de redes.

WEP

El primer método de encriptación más utilizado en las redes WiFi fue la encriptación WEP. WEP significa 'privacidad equivalente a la cableada' (del inglés *Wired Equivalent Privacy*), y está respaldada por casi todos los equipos 802.11a/b/g. Por cierto, WEP no es un nombre acertado porque la privacidad que da WEP no es para nada equivalente a la que dan las redes cableadas. WEP utiliza una clave compartida de 40-bits para encriptar los datos entre el punto de acceso y el cliente. La clave debe ingresarse en los AP, así como en cada uno de los clientes.

Cuando se habilita WEP, los clientes no pueden asociarse con el AP hasta que utilicen la clave correcta. Un fisgón escuchando en una red con WEP igual puede ver el tráfico y las direcciones MAC, pero los mensajes de los datos de cada paquete están encriptados.

Esto proporciona un mecanismo de autenticación, además de darle un poco de privacidad a la red.

WEP definitivamente no es la mejor solución de encriptación disponible. Por un lado, la clave WEP se comparte entre todos los usuarios, y si la misma está comprometida (es decir, si un usuario le dice a un amigo la contraseña, o un empleado abandona la organización) entonces cambiar la contraseña puede ser extremadamente difícil, ya que todos los AP y los dispositivos cliente deben cambiarla. Esto también significa que los usuarios legítimos de la red pueden escuchar el tráfico de los demás, ya que todos conocen la clave.

A menudo la clave es seleccionada sin mucho cuidado, haciendo posibles los intentos de ataques fuera de línea.

Aún peor, varias versiones de WEP son vulnerables mediante técnicas conocidas, haciendo aún más fácil atacar algunas redes. En pocas palabras, WEP no debería usarse más.

Para más detalles sobre la situación de la encriptación WEP, lea los siguientes artículos:

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
http://www.cs.umd.edu/~waa/wireless.pdf

Redes inalámbricas conmutadas (“*switched*”)

Una diferencia central entre las modernas redes Ethernet conmutadas y las inalámbricas es que estas últimas están construidas en un medio compartido. Se parecen más a los viejos concentradores (hubs) de red que a los modernos conmutadores en el sentido en que cada computador conectado a la red puede “ver” el tráfico de todos los demás usuarios.

Para monitorear todo el tráfico de red en un punto de acceso, uno simplemente puede sintonizar el canal que se está usando, poner la tarjeta de red en modo monitor y registrar cada trama.
Estos datos pueden tener valor directo para un fisgón (incluyendo datos de correo electrónico, de voz o registros de conversaciones en línea). Pueden también proporcionar contraseñas y otros datos privados comprometiendo aún más la seguridad de la red. WPA y 802.1X están diseñados para hacer que la red inalámbrica se comporte como red conmutada y no como compartida.

WPA

Otro protocolo de autenticación de la capa de enlace de datos es el Acceso Protegido a WiFi (WiFi Protected Access), o WPA. WPA fue creado para tratar de solucionar los problemas con WEP mencionados antes. WPA fue concebido como una solución interina compatible mientras se terminaba de desarrollar el estándar completo 802.11i (WPA2).

WPA y WPA2 pueden funcionar en combinación con el estándar de autenticación basado en puertos 802.1X (ver más adelante), pero también como WEP, utilizando un secreto compartido entre todos los clientes y el AP, el llamado Llave Pre-compartida (Pre Shared Key: PSK). La WiFi Alliance llama al WPA-PSK "WPA Personal", en contraposición a WPA Empresarial que se usa en combinación con 802.1X. En general, WPA proporciona una autenticación y privacidad considerablemente mejores que el estándar WEP, principalmente por que utiliza el Protocolo de Integridad de Clave Temporal (Temporary Key Integrity Protocol: TKIP) que cambia automáticamente y constantemente la clave.
Desafortunadamente, esa compatibilidad con la versión anterior del TKIP ha dado pie a algunos ataques contra el TKIP que permiten el descifrado de ciertos paquetes encriptados que, a la vez, pueden ser manipulados para ataques futuros.
Se puede encontrar más información en los artículos:

http://dl.aircrack-ng.org/breakingwepandwpa.pdf
http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf

La consecuencia de estos descubrimientos es que es más inteligente ir en la dirección de la nueva generación de los protocolos de acceso seguro a WiFi: WPA2.

WPA2-PSK

WPA2 es la implementación del estándar completo IEEE 802.11i.

La principal diferencia con WPA es el uso del Sistema de Encriptación Avanzada (Advanced Encryption System) AES, un estándar de encriptación (hasta ahora) no vulnerado, en lugar del TKIP.

Así que, el uso de WPA2 con AES se considera seguro !por ahora!

Resumen

La mayor desventaja de cualquiera de estos tres métodos de autenticación es que, a pesar de la fuerza de la encriptación, siguen funcionando sobre el esquema de un secreto compartido entre todos los clientes y el punto de acceso.

Estos métodos no permiten la identificación de usuarios individuales, y, francamente, un secreto compartido por potencialmente miles de usuarios apenas puede considerarse secreto.

Otro problema serio con las redes inalámbricas cuyo acceso es controlado por alguno de estos métodos es que sus usuarios son relativamente anónimos.
Aunque es cierto que cada dispositivo inalámbrico incluye una dirección MAC proporcionada por el fabricante, ya mencionamos que estas direcciones pueden ser cambiadas por medio de software. E incluso, cuando la dirección MAC es conocida, puede ser muy difícil calcular dónde está ubicado físicamente el usuario inalámbrico.

Efectos de multitrayectoria, antenas de gran ganancia, y las variadas características de los radios transmisores pueden hacer que sea imposible el determinar si un usuario inalámbrico está en la habitación vecina, o en un apartamento a 2 km de distancia.
La preocupación sobre la seguridad, la confiabilidad y la escalabilidad han dado origen a lo que se denomina comúnmente redes basadas en la identidad.

Redes basadas en la identidad

En este tipo de redes, los usuarios individuales son autenticados en lugar de compartir secretos con muchos usuarios.

Normalmente el sistema de autenticación verifica las credenciales del usuario comparándolas con una especie de directorio de la empresa o base de datos. Esto en general se hace usando el protocolo RADIUS, que originalmente fue diseñado para controlar el acceso a conjuntos de módems de discado, pero que es lo suficientemente versátil como para funcionar como protocolo de control genérico de acceso a redes.

Portales cautivos

Una herramienta común de autenticación utilizada en las redes inalámbricas es el *portal cautivo*. Este utiliza un navegador web estándar para darle al usuario inalámbrico la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso.

Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, cuando el usuario abre el navegador en su portátil es dirigido al portal. Al usuario, entonces, se le pide que acepte la política de uso, o que responda otras preguntas como nombre y contraseña y que haga clic en un botón de 'entrar' o tal vez ingresar números de un tique prepagado.

El usuario ingresa las credenciales, que son comprobadas por el punto de acceso u otro servidor en la red.

Cualquier otro acceso a la red se bloquea hasta tanto las credenciales sean verificadas.

Después de la verificación el computador recibirá una dirección DHCP. Y ahora podrá utilizar su navegador para explorar cualquier sitio en Internet.

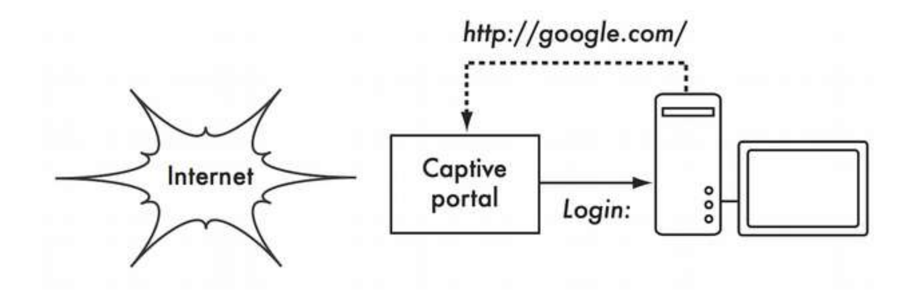


Figura SRI 1: El usuario solicita una página web y es redireccionado

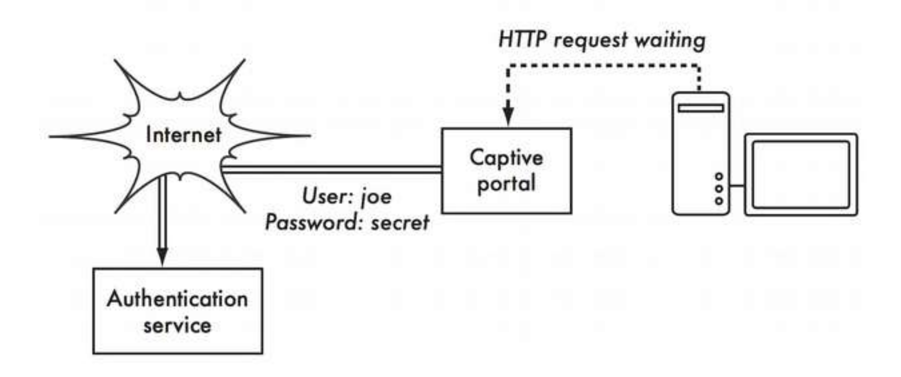


Figura SRI 2: Las credenciales del usuario son verificadas antes de otorgar el acceso a la red. El servidor de autenticación puede ser el punto de acceso mismo, otra máquina del la red local o un servidor en cualquier lugar en Internet

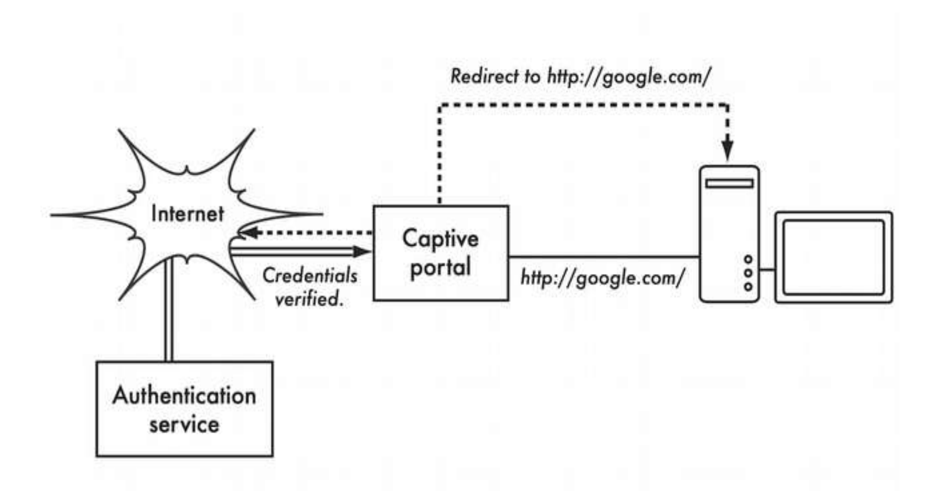


Figura SRI 3: Luego de la autenticación al usuario se le permite el acceso al resto de la red y comúnmente es redirigido al sitio originalmente solicitado, en este caso Google

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como único identificador, las cuales pueden ser fácilmente falseadas;

muchas implementaciones, por lo tanto, van a exigir que el usuario mantenga una ventana de conexión abierta. Puesto que los portales cautivos (igual que los basados en MAC o WEP) no ofrecen protección contra fisgones (usan un medio compartido) y son vulnerables a secuestros de sesión, no son una buena escogencia para verdaderamente garantizar el acceso a las redes exclusivamente a los usuarios legítimos.

Son más adecuadas para cafés, hoteles y otros lugares de acceso público donde se esperan usuarios casuales de la red. Otros defectos de estos portales es que dependen del uso de un navegador para la autenticación, lo que representa un paso adicional para los usuarios que sólo quieren consultar su correo o enviar un mensaje instantáneo, sin mencionar el hecho de que muchos dispositivos inalámbricos, como sensores, impresoras y cámaras, no tienen un navegador incorporado.
En redes públicas o semipúblicas, las técnicas de encriptación como WEP y WPA son realmente inútiles. Simplemente no hay forma de distribuir claves públicas o compartidas para el público en general sin comprometer la seguridad de esas claves.

En esas instalaciones, una simple aplicación como un portal cautivo proporciona un nivel de servicio intermedio entre completamente abierto y completamente cerrado.

Hay muchos vendedores y proyectos de código abierto que ofrecen las capacidades de portales cautivos. Para mencionar algunos:

- CoovaChilli, CoovaAP (http://coova.org/CoovaChilli/). Coova es el sucesor del proyecto desactivado Chillispot. Coova permite el uso de autenticación RADIUS.

- WiFi Dog (http://www.wifidog.org/). WiFi Dog provee un paquete muy completo de autenticación de portal cautivo en muy poco espacio (generalmente menos de 30 kB). Desde la perspectiva del usuario, no requiere de una ventana emergente (*pop-up*) ni de soporte javascript, lo que le permite trabajar en una amplia variedad de dispositivos inalámbricos.
- M0n0wall, pfSense (http://m0n0.ch/wall/); m0n0wall es un sistema operativo embebido completo basado en FreeBSD. Incluye un portal cautivo con soporte RADIUS, así como un servidor web PHP.

Muchos distribuidores generales de redes ofrecen alguna forma de portales cautivos, por ejemplo, Microtik, Cisco, Aruba, Aptilo.

802.1X

En las instalaciones de campus y de empresas, el esquema de autenticación para redes inalámbricas se basa en IEEE 802.1X. El 802.1X es un protocolo de capa 2 que puede ser usado para autenticación de redes inalámbricas o cableadas y, de hecho, engloba varias tecnologías. 802.1X describe la interacción entre el dispositivo cliente (Supplicant, en 802.1X) y el Punto de Acceso (Access Point) o Conmutador (Autenticador), así como la interacción entre el Punto de Acceso o Conmutador y un servidor RADIUS del administrador (Servidor de Autenticación), el cual, a su vez verifica las credenciales del usuario en un directorio de la empresa (o un archivo plano si fuera el caso.

Finalmente, 802.1X describe cómo transportar las credenciales del usuario desde el Supplicant al servidor de autenticación de manera transparente para el autenticador u otro dispositivo en la vía utilizando EAP, el Protocolo Extensible de Autenticación (*Extensible Authentication Protocol*).

La encriptación entre el supplicant y el autenticador puede realizarse rotando las claves WEP, WPA con TKIP, o WPA2 con AES. Por las razones expuestas en el párrafo sobre WEP, WPA-PSK y WPA2-PSK, se recomienda usar WPA2 con AES.

Probablemente, la característica más interesante del 802.1X es el uso de EAP. EAP define una forma genérica de encapsular las credenciales y transportarlas desde un supplicant (software cliente) a un servidor de autenticación (servidor RADIUS). Los así llamados métodos EAP definen cómo los métodos específicos de autenticación pueden ser encapsulados en EAP.

Hay métodos EAP para todos los tipos comunes de autenticación, como certificados, tarjetas SIM, nombres de usuario/clave, claves de un sólo uso y dispositivo de hardware.
Debido a problemas de distribución de claves o dispositivos y de su eventual revocación, la gran mayoría de instalaciones a gran escala usan lo que se llama métodos de EAP en túnel: autenticación basada en nombre de

usuario/clave de usuario usando un túnel TLS al servidor de autenticación a través del cual se transmiten el nombre del usuario y la clave.
La identidad del usuario empleada por el sobre TLS tiene comúnmente la forma anonymous@domain (lo que se llama la identidad externa), mientras que la identidad interna (dentro del túnel TLS) tiene la forma username@domain. Esta distinción es particularmente interesante para la itinerancia hacia las redes de otras organizaciones.
Es posible transportar las credenciales de autenticación de un usuario a través de Internet revelando únicamente la organización de origen del mismo (el dominio), pero eso es el tema de la próxima sección. Lo que ocurre en una autenticación 802.1X con método EAP es entonces lo siguiente:

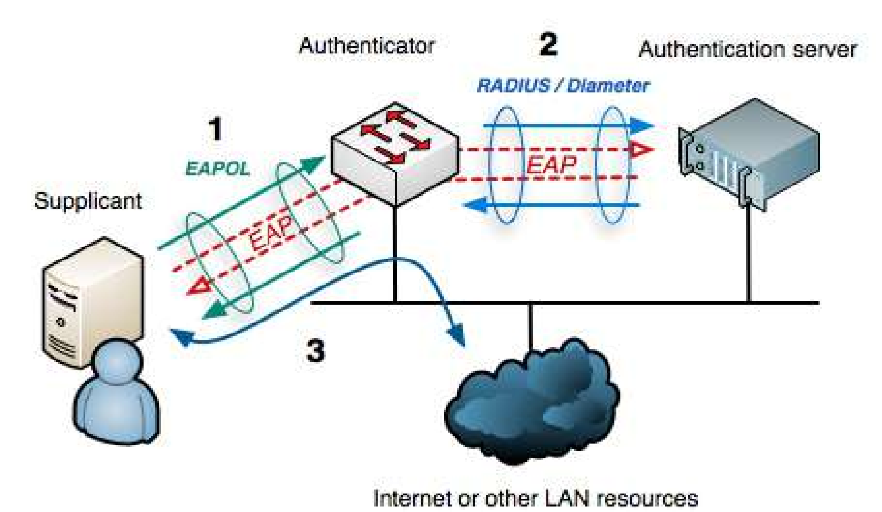


Figura SRI 4: El uso de 802.1X con túnel EAP para acceso a la red. (Cortesía de SURFnet)

El cliente se asocia al Punto de Acceso (autenticador).
El Punto de Acceso le pide al cliente (en la figura *Supplicant*) la autenticación.
El cliente le envía al AP un mensaje EAP que contiene un paquete TLS con una identidad externa anonymous@domain, y dentro del paquete TLS username@domain y la clave sobre el enlace 802.11 (EAP sobre LAN o EAPoL) El Punto de Acceso recibe el mensaje EAP, lo encapsula en RADIUS y lo envía al servidor RADIUS (servidor de autenticación).

El servidor RADIUS desencapsula el mensaje EAP y verifica las credenciales del usuario en un archivo del administrador (backend) del tipo archivo plano (flat file), un directorio LDAP, un Active Directory u otros.
Si las credenciales son válidas el servidor RADIUS le manda al Punto de Acceso un mensaje de aceptación (RADIUS Access Accept). El Punto de Acceso le da al usuario entonces el acceso a la LAN inalámbrica

El cliente hace una solicitud DHCP, obtiene una dirección IP y se conecta a la red.
Hay una cantidad de métodos de túnel EAP que operan básicamente de la misma manera. La diferencia va a estar en el respaldo en sistemas operativos comunes, la vulnerabilidad a ataques de diccionario y de "hombre en el medio"; y en el hecho de necesitar o no almacenar las claves no encriptadas en el servidor del administrador.

Los métodos de túnel EAP más instalados en la actualidad son EAP-TTLS (EAP Tunnelled Transport Layer Security) y PEAP (Protected EAP).

Ha habido implementaciones incompatibles de PEAP debido a desacuerdos entre los proponentes de PEAP (Apple, Cisco y Microsoft) que han resultado en una gran popularidad de TTLS. El hecho de que estas incompatibilidades se han resuelto mayormente y la carencia de soporte nativo para TTLS en un buen número de Sistemas Operativos (Apple iOS y variantes de Windows MS) han resultado en una creciente adopción de PEAP.
Un método EAP nuevo que está ganando terreno debido a sus propiedades de seguridad es el EAP-FAST. Este también ha sido escogido como la base para el nuevo método EAP de túnel (TEAP) que la IETF espera que sea el único adoptado.

Itinerancia (*roaming*) inter-organizacional

RADIUS tiene la interesante propiedad de que los mensajes RADIUS pueden ser delegados (*proxied*) a otros servidores RADIUS.
Eso significa que es posible que diferentes organizaciones permitan que los usuarios usen redes foráneas autenticándose en el servidor RADIUS de la organización de origen.
Cuando el servidor RADIUS de una organización A recibe una solicitud de autenticación por parte de anonymous@organisationB.org, aquél puede

remitir la solicitud al servidor RADIUS de la organización B en lugar de verificar las credenciales localmente. El servidor RADIUS de B, a su vez, puede verificar las credenciales y enviar el mensaje de "aceptación" de vuelta al servidor RADIUS de la organización A, que luego le comunica al Punto de Acceso que puede darle AP. Esto se llama acceso federado y permite la creación de despliegues grandes y ampliables, a la vez que permite a las organizaciones individuales aplicarles a los usuarios sus propias políticas de autenticación.
Mientras que delegar con RADIUS es posible en instalaciones de portal cautivo, donde realmente se luce es en los ambientes 802.1X/EAP. Como usa EAP las credenciales del usuario están protegidas de manera que sólo la organización original del usuario pueda verlas.

De esta manera se pueden crear grandes despliegues sin el riesgo de filtrado de credenciales y sin que los usuarios tengan que divulgar sus credenciales secretas en cada sitio web que encuentran.

Como un ejemplo, edurodam es una federación de acceso itinerante inalámbrico que amplía los conceptos expuestos anteriormente de manera que en lugar de tener conexiones RADIUS directas entre las organizaciones construye un sistema jerárquico de servidores RADIUS nacionales e internacionales, lo que permite a millones de estudiantes tener acceso a más de 5000 redes de campus en muchos países en todos los continentes excepto la Antártida.

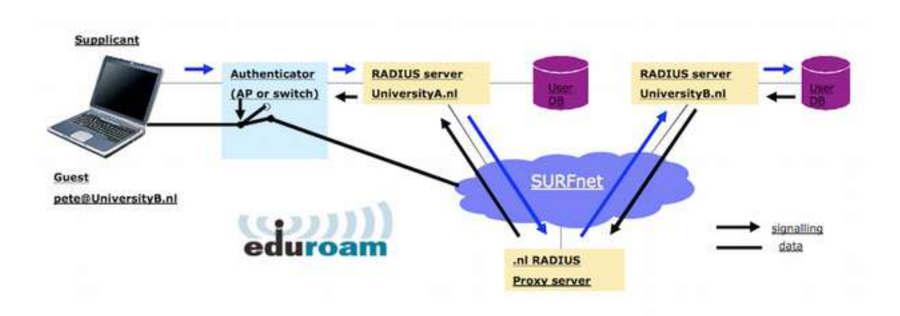


Figura SRI 5: La infraestructura de eduroam para itinerancia internacional en la academia

Encriptación de extremo a extremo a extremo

Debe notarse que mientras WEP, WPA-PSK y WPA2-PSK usan técnicas de encriptación para dar control de acceso y proteger contra intrusos estos sólo protegen el tráfico inalámbrico entre el cliente y el punto de acceso, no la parte cableada de la trayectoria de comunicación. Para proteger la comunicación de manipulación no autorizada o escuchas subrepticias, se necesita encriptación de extremo a extremo.
La mayoría de los usuarios están felizmente inconscientes de que sus correos privados, conversaciones de chat, e incluso contraseñas son enviados "en forma abierta" a través de docenas de redes poco confiables antes de que lleguen a su destino final en Internet. A pesar de estar equivocados, los usuarios esperan cierta privacidad cuando usan redes de computación. Esta privacidad puede lograrse incluso en redes poco confiables y en Internet. El único método de seguridad comprobado es la encriptación fuerte de punta a punta. Esta técnica trabaja bien incluso en redes públicas poco confiables donde hay intrusos que pueden estar oyendo o incluso manipulando los datos que proceden de un punto de acceso.
Para asegurar la privacidad, una buena encriptación de punta a punta debe tener estas características:

Autenticación verificada del extremo remoto

El usuario debe ser capaz de conocer sin ninguna duda que el extremo remoto es el que dice ser. Sin autenticación, un usuario puede darle datos importantes a cualquiera que afirme ser el servicio legítimo.

Métodos de encriptación fuerte

El algoritmo de encriptación debe ser expuesto al escrutinio del público, y no debe ser fácil de descifrar por un tercero. No hay seguridad en la oscuridad y una encriptación fuerte es incluso más fuerte cuando los algoritmos son ampliamente conocidos y sujetos a revisión por los pares.

Un buen algoritmo con una clave larga y adecuadamente protegida puede ofrecer encriptación imposible de descifrar aunque hagamos cualquier esfuerzo utilizando la tecnología actual. Hay que tener cuidado con los vendedores que le aseguran que sus encriptaciones comerciales con algoritmos secretos de fábrica son mejores que los que son abiertos y sujetos a escrutinio público.

Criptografía de clave pública

Aunque no es un requisito absoluto para la encriptación de extremo a extremo, el uso de criptografía de clave pública en lugar de una clave compartida puede asegurar que los datos personales de los usuarios se mantengan privados, aún si la clave de otro usuario del servicio se ve comprometida. Esto también resuelve ciertos problemas con la distribución de las claves a los usuarios a través de una red insegura.

Encapsulado de datos

Un buen mecanismo de encriptación de extremo a extremo protege tantos datos como sea posible. Esto puede ir desde cifrar una sencilla transacción de correo electrónico, a encapsular todo el tráfico IP, incluyendo búsquedas en servidores DNS y otros protocolos de soporte. Algunas herramientas de encriptación proveen un canal seguro que también pueden utilizar otras aplicaciones. Esto permite que los usuarios ejecuten cualquier programa que ellos quieran y aún así tengan la protección de una encriptación fuerte, aunque los programas no estén diseñados para la encriptación.

Note que la legislación sobre el uso de encriptación varía ampliamente de lugar en lugar. Algunos países pueden llegar a equiparar el uso de encriptación con el uso de municiones, y pueden exigir un permiso, la custodia de las claves privadas o prohibir su uso por completo. Antes de implementar cualquier solución que implique encriptación verifique que el uso de esta tecnología esté permitido en su comunidad.

En las siguientes secciones vamos a examinar algunas herramientas específicas que proveen una buena protección para los datos de sus usuarios.

TLS

La tecnología criptográfica de extremo a extremo más ampliamente usada es Transport Layer Security, conocida más sencillamente como TLS (o su antecesora SSL: Secure Sockets Layer).

TLS está incorporada virtualmente en todos los navegadores web y muchas otras aplicaciones. TLS usa criptografía de clave pública y una infraestructura de clave pública (PKI) confiable para asegurar la comunicación de los datos en la web.

Siempre que usted visita una URL web que comienza con https, usted está usando TLS.

La implementación de TLS incorporada a los navegadores incluye una colección de certificados de organizaciones, llamadas Autoridades de Certificación (CA). Una CA valida la identidad del usuario de red y/o proveedores, y se asegura de que son quienes dicen ser y le/les extiende un certificado que lo autentique.
Pero en lugar de hacerlo a través de un documento formal que se puede enmarcar, esto se hace a través del intercambio de claves de encriptación.
Por ejemplo, alguien que quiere un certificado para su página web envía una Solicitud de Certificado (Certificate Request: CR) "firmada" con una clave criptográfica creada especialmente para firmar esta solicitud.
Esta solicitud es enviada a la CA, que entonces "firma" la solicitud con su propia clave.
Estas son encriptadas en el certificado junto con el nombre exacto del sitio web para el cual el solicitante está pidiendo la validación del certificado.

Por ejemplo, WWW.AIPOTU.GOV, desde el punto de vista de la certificación no es lo mismo que AIPOTU.GOV. Cada sitio va a necesitar su propio certificado que presentará al buscador correspondiente para la transacción de autenticación HTTPS.
Si el dueño del dominio AIPOTU.GOV tiene sólo el certificado expedido para AIPOTU.GOV y no lo tiene también para WWW. AIPOTU.GOV, el usuario que acceda a la dirección "WWW" verá un mensaje de advertencia de certificado inválido para ese sitio. Esto puede confundir a los usuarios y con el tiempo, lleva a que estos esperen por parte de sus buscadores y como si fuera lo normal una advertencia de certificados TLS, cuando lo normal es completamente el caso opuesto.
Cuando usted accede a un sitio web que usa TLS, el buscador y el servidor intercambian certificados, como primer paso.
El buscador luego verifica que el nombre del host en el certificado proporcionado por el servidor concuerde con el nombre del host registrado en el servidor DNS; verifica también que el certificado no haya expirado ni haya sido revocado y que haya sido firmado por una autoridad de certificación. El servidor verifica opcionalmente la validez del certificado del buscador. Si los certificados son aprobados, ambas partes negocian una clave de sesión máster para proteger la sesión que se está abriendo.
Esta clave es entonces usada para encriptar todas las comunicaciones hasta que se desconecte el buscador. Este tipo de encriptación de datos es lo que se conoce como un túnel.

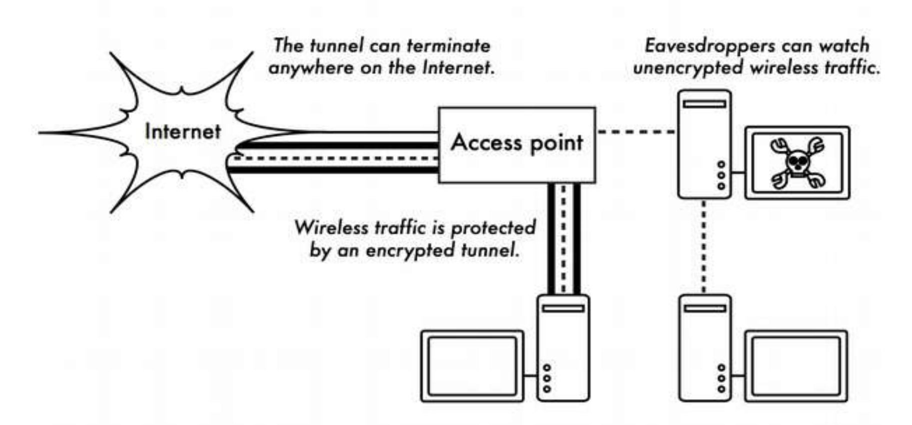


Figura SRI 6: Los fisgones tienen que violar la encriptación fuerte para inspeccionar el tráfico en un túnel encriptado. La conversación dentro del túnel es idéntica a cualquier conversación no encriptada

El uso de certificados con PKI no sólo protege la comunicación contra los fisgones sino previene de los ataques llamados "Hombre en el Medio" (Man-in-the-Middle, MitM). En un ataque MitM, un usuario malintencionado intercepta toda la comunicación entre un cliente y un servidor. Por medio de la presentación de certificados falsos tanto al servidor como al cliente, el usuario malintencionado puede sostener dos sesiones encriptadas simultáneas. Puesto que este usuario conoce las claves de ambas conexiones, le es muy fácil observar y manipular los datos que se transmiten entre el cliente y el servidor.

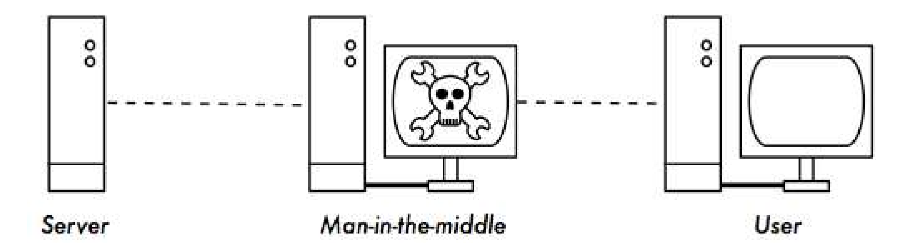


Figura SRI 7: El "hombre en el medio" efectivamente controla todo lo que ve el usuario, y puede grabar y manipular todo el tráfico. Sin una infraestructura de clave pública que verifique la autenticidad de las claves, la encriptación fuerte por sí sola no puede proteger contra este tipo de ataque

El uso de un buen PKI puede reducir considerablemente este tipo de ataque. Para tener éxito, el usuario malintencionado debería estar en posesión de un certificado firmado por una CA confiable de manera que pueda presentarlo al cliente y que este lo acepte como válido. Esto es posible si pueden engañar al usuario para que lo acepte o si el certificado CA ha sido falsificado.

Las autoridades de certificación (CA) tienen la gran responsabilidad de proteger sus sistemas y sus redes de accesos no autorizados y de usuarios malintencionados.
Si una CA fuera comprometida, el responsable del ataque podría llevar a cabo otros ataques MiTM contra cada usuario tratando de conectarse a los sistemas con un certificado emitido por la CA.

El atacante podría también emitir certificados falsos en respuesta a solicitudes de certificados legítimos, permitiendo la posibilidad de interceptar o interferir la comunicación encriptada entre buscadores y servidores.
Mientras que el compromiso de las CA era considerado algo remotamente posible hace un tiempo, al momento de escribir este artículo se han producido un número de incidencias que demuestran que esto ya no es cierto. Algunas compañías cuya actividad principal era la de funcionar como CA comerciales, han fracasado como resultado del compromiso de sus sistemas y de los certificados falsos emitidos en su nombre.

En Septiembre de 2011, la autoridad de certificados DigiNotar fue intervenida por piratas informáticos que produjeron la revocación de todos los certificados que habían emitido, lo que condujo a la quiebra de DigiNotar.
Estas violaciones no fueron el resultado de sofisticados criminales de la computación que emplearon ataques exóticos, sino el resultado de errores en la seguridad de la infraestructura general y en las políticas y procedimientos de seguridad.

Para finalizar, es bueno señalar que TLS no es de uso exclusivo de buscadores web. Algunos protocolos inseguros de correo electrónico como IMAP, POP y SMTP pueden asegurarse protegiéndolos con un túnel TLS.
La mayoría de los clientes de correo electrónico modernos admiten IMAPS y POPS (IMAP y POP seguros), así como SMTP protegido por TLS.

Si su servidor de correo no le da respaldo a TLS, puede asegurarlo con TLS usando un paquete como Stunnel (http://www.stunnel.org/). TLS puede usarse para dar seguridad efectiva a casi cualquier servicio ejecutable sobre TCP.

SSH

La mayoría de la gente considera SSH como un sustituto seguro para **telnet**, de la misma manera en que SCP y SFTP son los equivalentes seguros de RCP y FTP.

Pero SSH es mucho más que una consola remota encriptada. Por ejemplo, puede actuar también como un túnel de encriptación de uso general, o incluso para encriptar una red proxy (servidor web delegado).

Estableciendo de entrada una conexión SSH a un lugar confiable cerca de, (o incluso en) un servidor remoto, se puede dar protección a los protocolos inseguros contra fisgones o ataques.

Igual que TLS, utiliza criptografía fuerte de clave pública para la verificación del servidor remoto y el cifrado de los datos. En lugar de PKI usa una cache con clave de huella digital que es comprobada antes de autorizar la conexión.
Puede usar contraseñas y claves públicas para autenticación de los usuarios, y a través de su respaldo al sistema de módulos PAM (Pluggable Authentication Modules), puede también admitir otros métodos de autenticación.

Aunque esta técnica puede ser un tanto avanzada para muchos usuarios, los arquitectos de redes pueden usar SSH para cifrar el tráfico que pasa por enlaces no confiables como los enlaces punto a punto inalámbricos.

Puesto que las herramientas son gratuitas y compatibles con TCP estándar, cualquier usuario bien informado puede implementar por sí mismo conexiones SSH proporcionando su propia encriptación extremo a extremo sin intervención de un administrador.

OpenSSH (http://openssh.org/) es probablemente la implementación más popular en plataformas de tipo Unix.

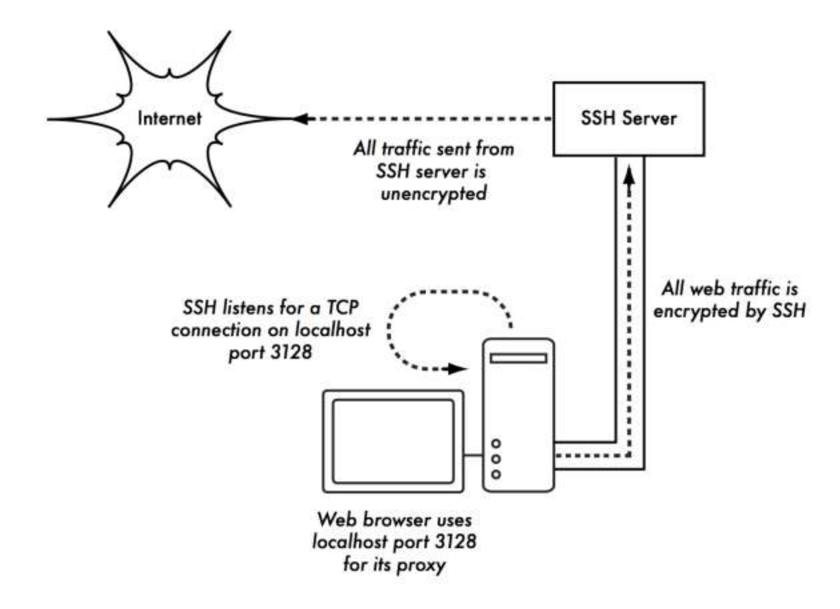


Figura SRI 8: El túnel SSH protege el tráfico web hasta el propio servidor SSH

Las implementaciones libres como Putty (http://www.putty.nl/) and WinSCP (http://winscp.net/) están disponibles para Windows.

OpenSSH también funciona en Windows mediante el paquete

Cygwin (http://www.cygwin.com/). Los ejemplos que siguen presuponen que usted está usando una versión reciente de OpenSSH. Para establecer un túnel cifrado desde un puerto en la computadora local hasta un puerto en el extremo remoto utilice la opción **-L**. Por ejemplo, supongamos que usted quiere reenviar el tráfico del *web proxy* en un enlace cifrado al servidor squid en *squid.example.net*. Reenvíe el puerto 3128 (el puerto *proxy* por omisión) utilizando este comando:

ssh -fN -g -L3128:squid.example.net:3128 squid.example.net

Las opciones **-fN** le ordenan a ssh que permanezca abierto en segundo plano después de conectarse.

La opción **-g** permite a otros usuarios en su segmento local que se conecten a la computadora local, y la utilicen para el cifrado sobre el enlace inseguro.

OpenSSH utilizará una clave pública para la autenticación si usted ya ha configurado una, o va a solicitarle su contraseña para conectarse al extremo remoto. Luego usted puede configurar su navegador web para conectarse al puerto 3128 del servidor local como su servidor proxy.

Todo el tráfico web será cifrado antes de la transmisión al sitio remoto. SSH también puede funcionar como un proxy dinámico SOCKS4 o SOCKS5. Esto le permite crear un web proxy encriptado sin necesidad de instalar squid. Tenga en cuenta que éste no será un proxy con memoria cache, simplemente cifra todo el tráfico:

```
ssh -fN -D 8080 remote.example.net
```

Configure su navegador web para utilizar SOCKS4 o SOCKS5 en el puerto local 8080, y listo. SSH puede cifrar datos en cualquier puerto TCP, incluyendo puertos utilizados para el correo electrónico.

También puede comprimir los datos, lo que puede hacer disminuir la latencia en enlaces de baja capacidad.

ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net

La opción **-C** habilita la compresión. Repitiendo múltiples veces la opción **-L** se pueden agregar tantas reglas de redirección de puertos como se quiera. Tenga en cuenta que para vincularse a un puerto local inferior a 1024, debe tener privilegios de administrador (root) en la máquina local.

Estos son solo algunos ejemplos de la flexibilidad de SSH. Al implementar claves públicas y utilizar el agente de reenvío ssh, puede automatizarse la creación de túneles cifrados a través de la red inalámbrica, y proteger sus comunicaciones con encriptación fuerte y autenticación.

OpenVPN

OpenVPN es una implementación VPN basada en encriptación SSL. Existen versiones tanto comerciales como una de fuente abierta. Existen versiones de Open VPN para un amplio rango de sistemas operativos, incluyendo Linux, Windows 2000/XP y superiores, OpenBSD, FreeBSD, NetBSD, y Mac OS X. Muchos usuarios encuentran Open VPN más fácil de entender y de configurar que los VPN IPSEC.

OpenVPN también tiene algunas desventajas, como por ejemplo una latencia bastante alta del tráfico en el túnel VPN.

Cierta cantidad de latencia no se puede evitar porque todo el cifrado/descifrado se hace en el espacio del usuario, pero si se utilizan computadoras relativamente nuevas en cada extremo del túnel, se puede minimizar. Si bien puede usar las tradicionales claves compartidas para la autenticación, OpenVPN se destaca realmente cuando se usa con certificados SSL y una autoridad de certificación. OpenVPN tiene algunas ventajas que lo hacen una buena opción para proveer seguridad de punta a punta.

Algunas de estas ventajas son:

- Se basa en protocolos de cifrado robustos y probados (SSL y RSA)
- Es relativamente fácil de configurar. Funciona en muchas plataformas diferentes
- Está bien documentado. Hay una versión de fuente abierta mantenida por la “Comunidad” y una versión comercial sujeta a pago.

OpenVPN necesita conectarse a un puerto único TCP o UDP en el extremo remoto. Una vez establecida la conexión, puede encapsular todos los datos en la capa de red, o en la capa de enlace de datos, de acuerdo con sus necesidades. Lo puede utilizar para crear conexiones VPN robustas entre máquinas individuales o simplemente utilizarlo para conectar enrutadores en redes inalámbricas inseguras. La tecnología VPN es un campo complejo, y dar más detalles está un poco más allá del alcance de esta sección. Es importante comprender dónde encajan las VPN en la estructura de su red, para proveer la mejor protección posible sin exponer su organización a problemas inesperados. Existen varios recursos en línea que se dedican a la instalación de OpenVPN en un servidor y un cliente. Se recomienda este artículo del Linux Journal:

http://www.linuxjournal.com/article/7949

así como el sitio oficial *HOWTO*:

http://openvpn.net/howto.html

Tor y Anonimizadores

Básicamente, Internet es una red abierta basada en la confianza. Cuando usted se conecta a un servidor web en Internet, su tráfico pasa a través de muchos enrutadores diferentes, pertenecientes a una gran variedad de instituciones, corporaciones y personas. En principio, cualquiera de esos enrutadores tiene la posibilidad de observar de cerca sus datos, mirando las direcciones de origen y destino, y muy a menudo el contenido de los datos.

Aún si sus datos están cifrados por medio de un protocolo seguro, su proveedor de Internet puede monitorear la cantidad de datos transferidos y el origen y destino de los mismos. A menudo esto es suficiente para componer un cuadro bastante completo de sus actividades en línea. La privacidad y el anonimato son importantes y están unidas estrechamente. Hay muchas razones válidas para considerar proteger su privacidad haciendo anónimo su tráfico en la red.

Supongamos que usted quiere ofrecer conectividad a Internet a su comunidad, instalando varios puntos de acceso para que la gente se conecte. Tanto si usted les cobra por el acceso como si no, existe siempre el riesgo de que la gente utilice la red para alguna actividad ilegal en su país o región.

Usted podría argumentarle al sistema legal que esa acción ilegal en particular no fue realizada por usted sino por cualquiera conectado a su red. Sin embargo, el problema legal puede evadirse elegantemente si no es técnicamente factible determinar adónde fue realmente dirigido su tráfico.

¿Y qué pasa con la censura on line? Publicar páginas web anónimamente puede ser necesario para evitar la censura del gobierno.

Existen herramientas que le permiten hacer anónimo su tráfico de formas relativamente sencillas. La combinación de Tor (http://www.torproject.org) y Privoxy (http://www.privoxy.org/) es una forma poderosa de manejar un servidor *proxy* local que pase su tráfico de Internet a través de varios servidores dispersos por la red, dificultando así seguir el rastro de la información.

Tor puede activarse en un PC local bajo Microsoft Windows, Mac OSX, Linux y una variedad de BSD, haciendo que el tráfico desde el navegador a esa máquina en particular sea anónimo. Tor y Privoxy también pueden instalarse en una pasarela (*gateway*), o también en un pequeño punto de acceso embebido (como el Linksys WRT54G) donde se proporciona anonimato automáticamente para todos los usuarios de la red.

Tor funciona haciendo “rebotar” repetidamente sus conexiones TCP a través de varios servidores esparcidos en Internet, y envolviendo la información de enrutamiento en varias capas cifradas (de ahí el término enrutamiento 'cebolla'), que se van desechando cuando el paquete se mueve por la red.

Esto significa que, en cualquier punto en la red, la dirección de la fuente y la del destino no pueden relacionarse una con la otra. Esto hace que el análisis del tráfico sea extremadamente difícil.

La necesidad del proxy de privacidad Privoxy en combinación con Tor se debe al hecho de que las solicitudes de resolución de nombres (solicitudes DNS) en la mayoría de los casos no pasan a través del servidor proxy, y alguien que esté analizando su tráfico puede ser capaz de ver que usted está intentando acceder a un sitio específico (por ejemplo google.com) por el hecho de que usted envía una solicitud DNS para traducir google.com a la dirección IP apropiada. Privoxy se conecta a Tor como un proxy SOCKS4a, el cual usa nombres de servidores (no direcciones IP) para entregar sus paquetes al destino deseado.

En otras palabras, utilizar Privoxy con Tor es una forma simple y efectiva de prevenir el análisis del tráfico a partir de la relación de su dirección IP con los servicios que utiliza en línea. Combinado con protocolos de cifrado seguros (como los que hemos visto en este capítulo), Tor y Privoxy proporcionan un alto nivel de anonimato en Internet.

PLANIFICACIÓN E INSTALACIÓN

10. PLANIFICANDO EL DESPLIEGUE

Cálculo de la capacidad

Para calcular la capacidad es importante entender que la velocidad declarada de un dispositivo inalámbrico (la llamada tasa de datos) se refiere a la tasa a la cual los radios intercambian símbolos, no al caudal utilizable que se puede aprovechar. El caudal (throughput) es también conocido como la capacidad del canal, o simplemente ancho de banda (sin embargo, el término es muy diferente al ancho de banda de la radio!).

El ancho de banda cuando se refiere a caudal se mide en Mbps, pero la definición estricta del ancho de banda se mide en MHz. Por ejemplo, un enlace único 802.11g puede usar radios de 54 Mbps, pero va a proporcionar sólo hasta 22 Mbps del caudal real. El resto es tara (*overhead*) que los radios necesitan para coordinar sus señales utilizando el protocolo 802.11g.

Note que el caudal es una medida de bits en el tiempo. 22 Mbps significa que en un segundo dado, hasta 22 megabits pueden ser enviados de un extremo al otro del enlace. Si los usuarios intentan forzar más de 22 megabits a través del enlace, va a tomar más tiempo de un segundo.

Puesto que los datos no pueden ser enviados inmediatamente se colocan en una cola y se transmiten tan pronto como sea posible.
Esto incrementa el tiempo necesario para que los bits más recientes en la cola atraviesen el enlace. El tiempo que le toma a los datos atravesar el enlace se llama latencia, y a una alta latencia se le conoce usualmente como retardo.

Su enlace va a la larga a enviar todos el tráfico en la cola, pero sus usuarios probablemente se van a quejar a medida que el retardo se incrementa
¿Qué tanto caudal van a necesitar realmente sus usuarios?
Depende de cuántos usuarios haya, y de cómo utilicen el enlace inalámbrico.
Distintas aplicaciones de Internet van a necesitar diferentes caudales.

Aplicaciónes	**Requisito / Usuario**	**Notas**
Mensajes de texto/ IM	< 1 kbps	Como el tráfico es infrecuente y asíncrono, IM tolera latencia alta.
Correo Electrónico	1 a 100 kbps	Igual que con IM, el email es asíncrono e intermitente así que va a tolerar latencia. Archivos anexos grandes, virus, y spam incrementan significativamente el uso de ancho de banda. Note que los servicios de email basados en web (como Yahoo y Hotmail) deben ser considerados como navegación en web y no como email.
Navegación Web	50 - 100+ kbps	Los navegadores web sólo usan la red cuando los datos son solicitados. La comunicación es asíncrona, así que una buena cantidad de retardo puede tolerarse. A medida que los navegadores solicitan más datos (imágenes grandes, descargas largas, etc.) el uso de ancho de banda aumenta considerablemente.
Audio en tiempo real (streaming)	96 - 160 kbps	Cada usuario de audio en tiempo real va a usar una cantidad considerable y constante de ancho de banda por todo el tiempo en que esté escuchando. Puede tolerar latencia transitoria utilizando grandes cantidades de memoria del cliente. Pero períodos largos de retardo van a producir "saltos" en el audio o fallos completos de la sesión.
Voz sobre IP (VoIP)	24 - 100+ kbps	Igual que con el audio en tiempo real, la VoIP compromete un ancho de banda constante por cada usuario durante el tiempo de la llamada. Pero con la VoIP, el ancho de banda se usa aproximadamente de manera igual en ambas direcciones. La latencia en una conexión VoIP es una molestia inmediata para los usuarios. Los retrasos más largos de unos pocos milisegundos son inaceptables en VoIP.
Video en tiempo real (streaming)	64 - 200+ kbps	Igual que con el audio en tiempo real, alguna latencia intermitente se puede evitar usando memoria del cliente. El video en tiempo real necesita un caudal elevado y baja latencia para funcionar adecuadamente.
Aplicaciones de compartir archivos (peer-to-peer)	0- infinito Mbps	Mientras que las aplicaciones peer-to-peer toleran cierta latencia, tienden a usar todo el caudal disponible para transmitir datos al mayor número de clientes posible, en el menor tiempo posible. El uso de estas aplicaciones va a ocasionar problemas de latencia y caudal para el resto de de los usuarios de la red a menos que usted use un control de tráfico muy cuidadoso.

Para calcular el caudal necesario que va a necesitar para su red, multiplique el número esperado de usuarios por los requisitos de las aplicaciones que probablemente usarán.

Por ejemplo, 50 usuarios que comúnmente buscan en la red consumirán 2.5 a 5 Mbps o más de caudal en los tiempos pico y tolerarán alguna latencia.

Pero, 50 usuarios usando simultáneamente VoIP necesitarán 5 Mbps o más de caudal en ambas direcciones con baja latencia. Puesto que el equipo inalámbrico 802.11g es half duplex (es decir, sólo transmite o recibe, pero no ambos a la vez) usted debería de igual manera duplicar el caudal necesario hasta un total de 10 Mbps.

Su enlace inalámbrico debe proporcionar esa capacidad cada segundo o la conversación se retrasa.
Puesto que es improbable que todos los usuarios usen la conexión exactamente al mismo tiempo, es práctica común sobresuscribir el caudal disponible usando algún factor (es decir, permitir más usuarios de los que el máximo ancho de banda disponible puede tolerar).

Sobresuscribir usando un factor de 5 a 10 es bastante común.

El monitoreo cuidadoso del caudal en toda su red le va a permitir la planificación de cuándo actualizar las diferentes partes de la misma y calcular cuántos recursos adicionales va a necesitar.

Cálculo del presupuesto del enlace

El proceso de determinar si un enlace es viable se denomina ***cálculo del presupuesto del enlace*** o balance de potencia
y puede ser hecho manualmente o usando herramientas especializadas.

Un sistema de comunicación básico consiste en dos radios, cada uno con su antena y separados por el trayecto a ser cubierto como se muestra en la siguiente figura.

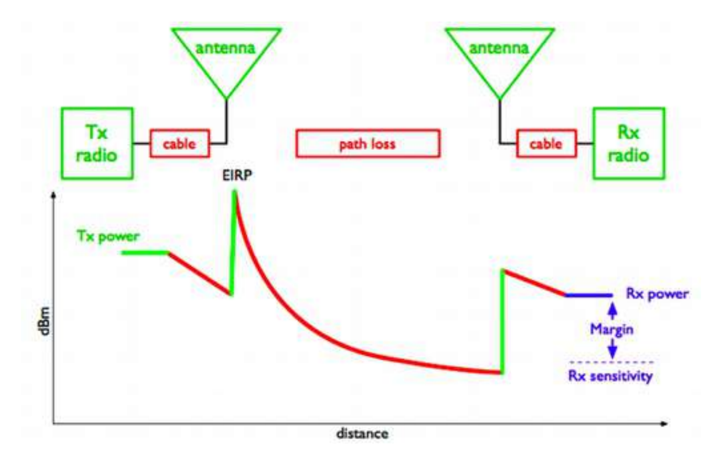


Figura PD 1: Componentes de un Sistema Básico de Comunicación

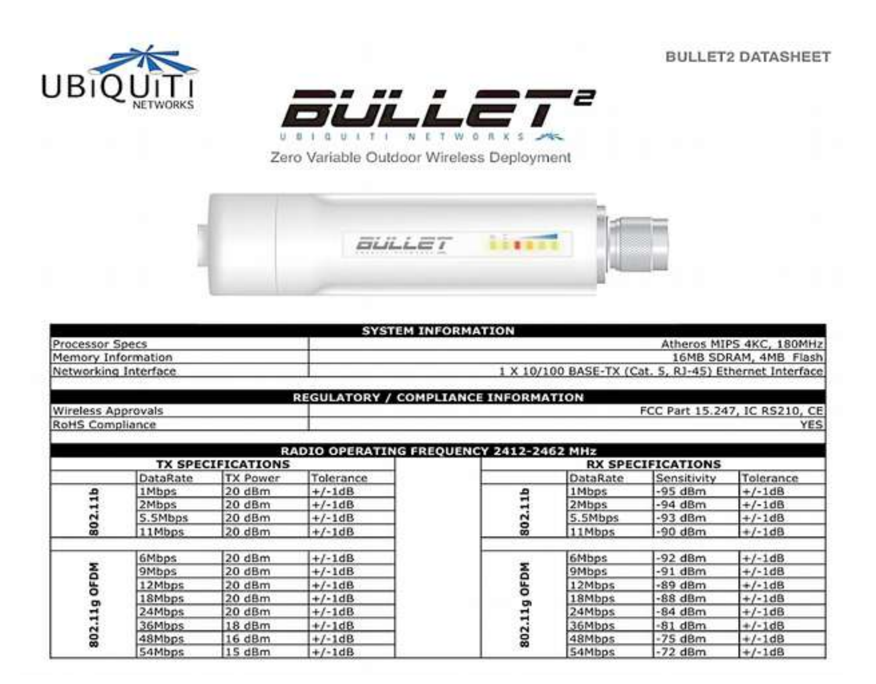
La señal recibida tiene que estar por encima de un cierto nivel mínimo para que la comunicación pueda ser confiable.

El que las señales puedan o no ser transmitidas entre los radios va a depender de las características del equipo y de la disminución de la señal debido a la distancia, lo que se llama ***pérdida de trayectoria***. En este sistema algunos parámetros pueden ser modificados (el equipo empleado, por ejemplo) mientras que otros permanecen fijos (la distancia entre los radios). Comencemos examinando los parámetros modificables.

1. Las características del equipo que se deben considerar cuando se calcula el presupuesto del enlace son:

Potencia de Transmisión (TX). Se expresa en milivatios o en dBm. La potencia de transmisión a menudo depende de la tasa de transmisión. La potencia TX de un dispositivo dado debería especificarse en los manuales del fabricante.

A continuación damos un ejemplo donde se puede observar que al usar 802.11g hay una diferencia de 5 dB en la potencia de salida cuando se usa 6 Mbps o 54 Mbps.



SYSTEM INFORMATION	
Processor Specs	Atheros MIPS 4KC, 180MHz
Memory Information	16MB SDRAM, 4MB Flash
Networking Interface	1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface

REGULATORY / COMPLIANCE INFORMATION	
Wireless Approvals	FCC Part 15.247, IC RS210, CE
RoHS Compliance	YES

RADIO OPERATING FREQUENCY 2412-2462 MHz

TX SPECIFICATIONS			
	DataRate	TX Power	Tolerance
802.11b	1Mbps	20 dBm	+/-1dB
	2Mbps	20 dBm	+/-1dB
	5.5Mbps	20 dBm	+/-1dB
	11Mbps	20 dBm	+/-1dB
802.11g OFDM	6Mbps	20 dBm	+/-1dB
	9Mbps	20 dBm	+/-1dB
	12Mbps	20 dBm	+/-1dB
	18Mbps	20 dBm	+/-1dB
	24Mbps	20 dBm	+/-1dB
	36Mbps	18 dBm	+/-1dB
	48Mbps	16 dBm	+/-1dB
	54Mbps	15 dBm	+/-1dB

RX SPECIFICATIONS			
	DataRate	Sensitivity	Tolerance
802.11b	1Mbps	-95 dBm	+/-1dB
	2Mbps	-94 dBm	+/-1dB
	5.5Mbps	-93 dBm	+/-1dB
	11Mbps	-90 dBm	+/-1dB
802.11g OFDM	6Mbps	-92 dBm	+/-1dB
	9Mbps	-91 dBm	+/-1dB
	12Mbps	-89 dBm	+/-1dB
	18Mbps	-88 dBm	+/-1dB
	24Mbps	-84 dBm	+/-1dB
	36Mbps	-81 dBm	+/-1dB
	48Mbps	-75 dBm	+/-1dB
	54Mbps	-72 dBm	+/-1dB

Figura PD 2: Hoja de especificación de Ubiquiti Bullet2

Ganancia de las Antenas

Las antenas son dispositivos pasivos que crean el efecto de amplificación gracias a su forma física. Las antenas tienen las mismas características cuando reciben que cuando transmiten. De esta manera, una antena de 12 dBi es simplemente una antena de 12 dBi sin especificar si es en el modo de transmisión o de recepción. Algunos valores típicos son: las antenas parabólicas tienen una ganancia entre 19-24 dBi: las omnidireccionales entre 5-12 dBi; y las sectoriales grosso modo de 12-15 dBi de ganancia.

Nivel Mínimo de señal recibida (Received Signal Level: RSL), o simplemente la sensibilidad del receptor. El RSL mínimo se expresa siempre como dBm negativos (-dBm) y es el nivel más bajo de señal que el radio puede distinguir. El RSL mínimo depende de la tasa de transmisión y como regla general la tasa más baja (1 Mbps) tiene la sensibilidad más alta. El mínimo va a estar generalmente en el rango de los -75 a -95 dBm.

Al igual que la potencia TX, las especificaciones debería proporcionarlas el fabricante del equipo. En la hoja de datos que se presentó arriba se puede ver que hay una diferencia de 20 dB en la sensibilidad del receptor, con -92 dBm a 6 Mbps y -72 dBm a 54 Mbps.

!No olvide que una diferencia de 20 dB significa un cociente de 100 en términos de potencia!

Pérdidas en los Cables. Parte de la energía de la señal se pierde en los cables, los conectores y otros dispositivos desde los radios a las antenas. La pérdida depende del tipo de cable usado y de su longitud.
La pérdida de señal para cables coaxiales cortos incluyendo los conectores es bastante baja, en el rango de los 2-3 dB. Es mejor usar cables lo más cortos posible. Los equipos ahora suelen traer antenas empotradas y por lo tanto los cables son muy cortos.

2. Cuando se calcula la pérdida en la trayectoria, algunos aspectos deben considerarse. Se deben tener en cuenta ***la pérdida en espacio libre, la atenuación y la dispersión.***

Pérdida en espacio libre.
La dispersión geométrica del frente de onda, conocida generalmente como pérdida en el espacio libre, disminuye la potencia de la señal. Ignorando todo lo demás, cuanto más lejanos estén los dos radios, más pequeña es la señal debido a la pérdida en el espacio libre. Esto es independiente del medio ambiente; depende sólo de la distancia. Esta pérdida ocurre porque la energía de la señal irradiada se expande en función de la distancia desde el transmisor.

Usando los decibeles para expresar la pérdida y usando una frecuencia genérica f, la ecuación para la pérdida en el espacio libre es:

$$L_{fsl} = 32.4+20*log_{10}(D)+20*log_{10}(f)$$

donde L_{fsl} se expresa en dB; ***D*** en kilómetros y **f** en MHz.

Cuando llevamos a una gráfica la pérdida en espacio libre versus la distancia, se obtiene una figura como la PE 3. Se debería notar que la diferencia entre usar 2400 MHz y 5300 MHz es de 6 dB en términos de pérdida en espacio libre. De manera que una frecuencia más alta da una pérdida más alta, lo que se contrarresta usualmente con una ganancia mayor de la antena parabólica. Una antena parabólica operando a 5 GHz es 6 dB más potente que otra con las mismas dimensiones que opera a 2.4 GHz para las mismas dimensiones de la antena.

Si tenemos dos antenas con 6 dB más de ganancia en cada extremo se obtienen 6 dB netos de ventaja cuando se migra de 2.4 a 5 GHz.

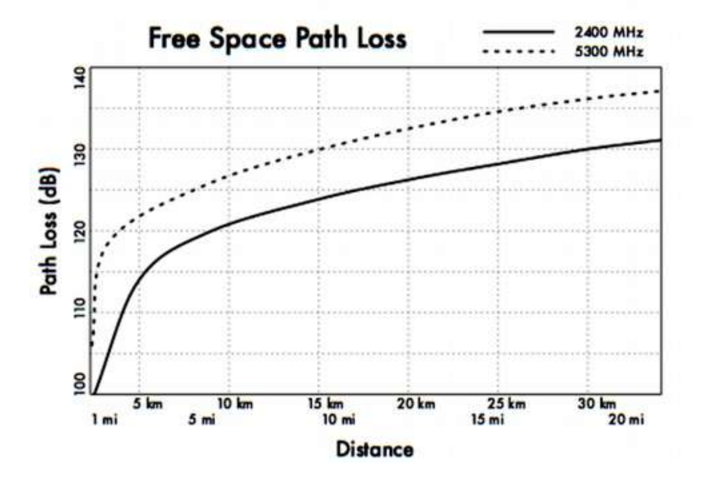


Figura PD 3: Gráfico de cálculo de pérdida de la trayectoria en el espacio libre

Atenuación

El segundo factor que contribuye con la pérdida en la trayectoria es la atenuación. Esta se produce cuando parte de la potencia de la señal es absorbida cuando pasa a través de objetos sólidos como árboles, paredes, ventanas, y pisos de los edificios.

La atenuación puede variar mucho dependiendo de la estructura del objeto que atraviesa la señal, y es muy difícil de cuantificar.

Dispersión

A lo largo del trayecto del enlace la potencia de RF (radio frecuencia) deja la antena transmisora y se dispersa. Una parte de la de la potencia de RF alcanza a la antena receptora directamente, mientras otra parte rebota en la tierra. Parte de esa potencia que rebota alcanza la antena receptora. Puesto que la señal reflejada tiene un espacio más largo por recorrer, llega a la antena receptora más tarde que la señal directa. Este efecto se llama ***multitrayectoria***, o dispersión de la señal. En algunos casos las señales reflejadas se suman y no causan problema. Cuando se suman en contrafase, la señal recibida es casi inútil. En algunos casos, la señal en la antena receptora puede ser anulada por las señales reflejadas.

A esto se conoce como desvanecimiento extremo o anulación. Hay una técnica simple utilizada para resolver problemas de multitrayectoria llamada diversidad de antena. Esta consiste en añadir una segunda antena al radio.

Si dos señales se suman en contrafase en un punto, anulándose, no van a anularse en otro punto cercano. Si hay dos antenas, por lo menos una de ellas debería ser capaz de recibir una señal utilizable, incluso si la otra está recibiendo una muy debilitada. En dispositivos comerciales se usa diversidad de antenas conmutadas: antenas múltiples en múltiples entradas con un receptor único.

Se pasa al receptor la señal de la antena que tenga la señal más fuerte.
Cuando se transmite, el radio usa la última antena utilizada para la recepción. La distorsión dada por multitrayectoria degrada la capacidad del receptor para recobrar la señal de una manera parecida a la pérdida de la señal.

Unir todos estos parámetros conduce al ***cálculo del presupuesto del enlace***. Si se están usando radios diferentes en los dos extremos del enlace, la pérdida en la trayectoria debe calcularse dos veces, una por cada dirección (usando la potencia apropiada TX, la potencia RX, la ganancia TX de antena, y la ganancia RX de la antena para cada cálculo).
Al sumar todas las ganancias y restar todas las pérdidas tenemos:

TX Potencia	*Radio 1*
+Ganancia de Antena	*Radio 1*
-Pérdida en Cables	*Radio 1*
+Ganancia de Antena	*Radio 2*
-Pérdida en Cables	*Radio 2*
=Ganancia Total	

Al restar la Pérdida en la Trayectoria de la Ganancia Total:

Ganancia Total - Pérdida en la Trayectoria = Nivel de la Señal en el extremo receptor del enlace

Si el nivel de la señal resultante es mayor que la sensibilidad del receptor, entonces !el enlace es viable! La señal recibida es lo suficientemente potente como para que el radio la utilice.

Recuerde que el RSL mínimo se expresa siempre en dBm negativos, así que -56 dBm es mayor que -70 dBm.

En un trayecto dado, la variación de pérdida en trayectoria en un período de tiempo puede ser grande, así que un cierto margen debe ser tomado en cuenta. Este margen es la cantidad de señal por encima de la sensibilidad del radio que debería recibirse para garantizar un enlace de radio estable y de alta calidad incluso en mal tiempo u otras perturbaciones atmosféricas.

Un margen de 10 a 15 dB está bien. Para permitir cierto espacio para la atenuación y la multitrayectoria en la señal de radio recibida, un margen de 20 dB debería ser bastante seguro.

Una vez que se haya calculado el presupuesto del enlace en una dirección, hay que repetir el cálculo en la otra dirección. Substituya la potencia de transmisión por la del segundo radio y compare el resultado con el nivel mínimo de la señal recibida del primer radio.

Ejemplo de cálculo del presupuesto del enlace

Como ejemplo, queremos estimar la viabilidad de un enlace de 5 km con un punto de acceso y un radio cliente.

- El punto de acceso está conectado a una antena omnidireccional con una ganancia de 10 dBi, mientras que el cliente está conectado a una antena direccional de 14 dBi.
- La potencia de transmisión del AP es de 100 mW (ó 20 dBm) y su sensibilidad de -89 dBm.
- La potencia de transmisión del cliente es 30 mW (ó 15 dBm) y su sensibilidad es de -82 dBm.
- Los cables son cortos, así que calculamos una pérdida de 2 dB en cada lado.

Empecemos por calcular el presupuesto del enlace desde el AP al cliente, como se muestra en la Figura PD 4.

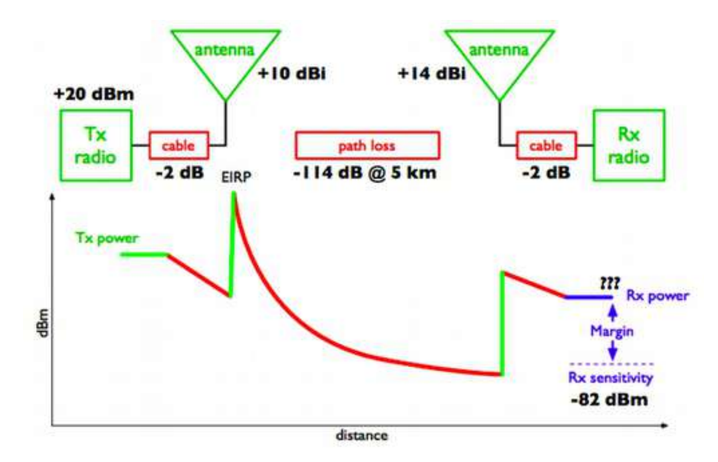


Figura PD 4: Cálculo del presupuesto del enlace desde AP al cliente

Sumando todas las ganancias y restando las pérdidas desde AP hasta el cliente nos da:

20 dBm	*TX Potencia del Radio 1*
+10 dBi	*Ganancia de la Antena del Radio 1*
-2 dB	*Pérdida en el Cable del Radio 1*
+14 dBi	*Ganancia de la Antena del Radio 2*
-2 dB	*Pérdida en el Cable del Radio 2*
40 dB =	*Ganancia Total*
-114 dB	*Pérdida en el espacio libre @ 5 km*
-73 dBm	*Nivel de Señal Recibida*
-(- 82) dBm	*Sensibilidad del Cliente*
8 dB	*Margen del enlace*

La pérdida en el espacio libre de un enlace de 5 km, a la frecuencia de 2.4 GHz es de -114 dB. Al restar la pérdida en el trayecto de la ganancia total:

40 dBm - 114 dB = -74 dBm

Puesto que -74 dBm es mayor que la sensibilidad mínima del receptor del cliente (-82 dBm), el nivel de la señal es suficiente para que el radio cliente pueda oír el punto de acceso.

Hay solamente 8 dB de margen (82 dBm —74 dBm) que van a ser suficientes para funcionar bien con buen tiempo, pero puede que no lo sea para funcionar en condiciones climáticas extremas.
Lo siguiente es calcular el enlace desde el cliente hasta el punto de acceso, como se muestra a continuación.

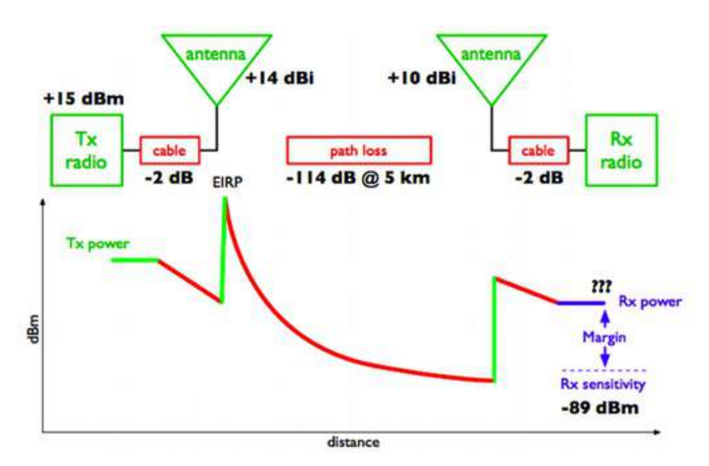


Figura PD 5: Cálculo del presupuesto del enlace desde el cliente a AP

15 dBm	*TX Potencia del Radio 2*
+14 dBi	*Ganancia de Antena del Radio 2*
-2 dB	*Pérdida en el Cable del Radio 2*
+10 dBi	*Ganancia de Antena del Radio 1*
-2 dB	*Pérdida en el Cable del Radio 1*
______	
35 dB	*Ganancia Total*
-114 dB	*Pérdida en el Espacio Libre @ 5 km*
______	
-78 dBm	*Nivel de Señal Recibida*
-(-89) dbBm	*Sensibilidad del Cliente*
______	
10 dB	*Margen del enlace*

Obviamente, la pérdida en el trayecto es la misma en el viaje de vuelta. Así que el nivel de la señal receptora en el extremo del punto de acceso es:

35 dBm- 114 dB = -79 dBm

Puesto que la sensibilidad de recepción del AP es de -89 dBm, vamos a tener un margen de 10 dB (89 dBm —79 dBm). En general, este enlace va a funcionar bien.
Empleando una antena de 24 dBi en el extremo del cliente, en lugar de una de 14 dBi, obtendremos una ganancia adicional de 10 dBi en ambas direcciones del enlace (recuerde que la ganancia de la antena es recíproca).

Una opción más cara sería la de usar radios de mayor potencia en cada extremo del enlace, pero nótese que al añadir un amplificador o una tarjeta de alta potencia en uno solo de los extremos no se va a lograr una mayor calidad global del enlace.

Tablas para calcular el presupuesto del enlace

Para calcular el presupuesto del enlace, simplemente aproxime la distancia de su enlace y rellene las tablas siguientes:

Pérdida de Trayectoria en el Espacio Libre a 2.4 GHz

Distancia (m)	100	500	1000	3000	5000	10000
Pérdida (dB)	80	94	100	110	114	120

Ganancia de la Antena

Antena Radio 1	+ Antena Radio 2	= Ganancia Total de la Antena

Pérdidas:

Radio 1 + Pérdida en los Cables (dB)	Radio 2 + + Pérdida en los Cables (dB)	Pérdida de Trayectoria en Espacio Libre (dB)	= Pérdida Total (dB)

Presupuesto del Enlace. Radio 1 ---> Radio 2:

Potencia TX del Radio 1	+ Ganancia de la Antena	- Pérdida Total	= Señal	> Sensibilidad del Radio 2

Presupuesto del Enlace. Radio 2 ---> Radio 1:

Potencia TX del Radio 2	+ Ganancia de la Antena	- Pérdida Total	= Señal	> Sensibilidad del Radio 1

Si la señal recibida es mayor que la intensidad mínima de señal recibida en ambas direcciones del enlace, así como cualquier ruido recibido en la trayectoria, el enlace es posible.

Software para la planificación del enlace

Si bien calcular el presupuesto de un enlace a mano es sencillo, hay algunas herramientas que ayudan a automatizar el proceso. Además de calcular la pérdida en el espacio libre, esas herramientas van a tomar en cuenta otros factores relevantes (como absorción de los árboles, efectos del terreno, clima, e incluso la estimación de las pérdidas en el trayecto en áreas urbanas).

La mayoría de las herramientas comerciales son muy caras y a menudo son diseñadas para ser usadas en un hardware específico.

En la sección siguiente vamos a discutir una herramienta gratuita llamada Radio Mobile.

Radio Mobile

Radio Mobile es una herramienta para el diseño y simulación de sistemas inalámbricos.

Predice las prestaciones de radioenlaces utilizando información acerca del equipo y un mapa digital del área. Es un software de dominio público pero no de fuente abierta. Radio Mobile usa un modelo digital de elevación del terreno para el cálculo de la cobertura e indica la intensidad de la señal recibida en varios puntos a lo largo del trayecto.

Construye automáticamente un perfil entre dos puntos en el mapa digital mostrando el área de cobertura y la primera zona de Fresnel.

Un ejemplo se presenta en la figura PE 6 a continuación.

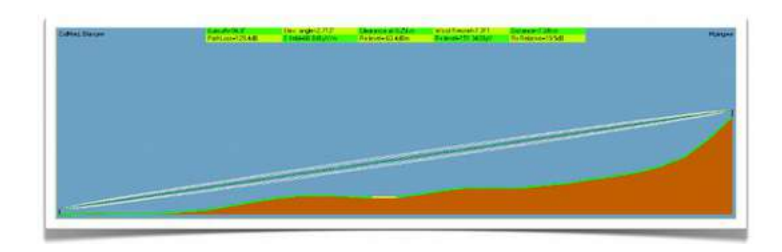


Figura PD 6: Simulación en Radio Mobile que muestra una elevación digital del terreno y la primera zona de Fresnel

Durante la simulación comprueba la línea visual y calcula la Pérdida en el Espacio, incluyendo pérdidas debidas a los obstáculos.
Es posible crear redes de diferentes topologías master/slave, punto a punto y punto a multipunto.
El software calcula el área de cobertura desde la estación base en un sistema punto a multipunto.
Trabaja para sistemas que tienen frecuencias de 20 MHz a 200 Ghz.

Los mapas de elevación digital (Digital elevation maps: DEM) están disponibles gratuitamente desde variadas fuentes para la mayor parte del mundo.

Los DEM no muestran las líneas costeras u otras marcas morfológicas fácilmente identificables, pero pueden combinarse fácilmente con otro tipo de datos (como fotos aéreas o cartas topográficas) para obtener una representación más útil y rápidamente reconocible. Usted puede digitalizar sus propios mapas y combinarlos con DEM.
Los mapas de elevación digitales pueden combinarse con mapas escaneados, fotos satelitales y servicios de mapas de Internet (como Google Maps) para obtener esquemas precisos de predicción.
Hy dos versiones de Radio Mobile.
Una versión que funciona en Windows y otra en línea accesible mediante una interfaz web.

Estas son sus diferencias:

Versión Web:

- funciona en cualquier máquina (Linux, Mac, Windows, tableta, teléfono, etc.)
- no precisa de descargas grandes. Puesto que trabaja online, los datos se almacenan en el servidor y sólo aquellos datos necesarios se descargan
- registra las sesiones. Si usted ejecuta una simulación y vuelve a entrar después de un tiempo, todavía va a encontrar la simulación y los resultados
- es más fácil de usar, sobre todo para principiantes.
- necesita conexión. No es posible hacer una simulación offline.
- como ha sido desarrollado para los radioaficionados funciona solamente en ciertas bandas de frecuencia. Como ejemplo, no es posible simular enlaces a 5.850 GHz, sino sólo a 5.825 GHz.

Versión Windows:

- funciona offline. Una vez descargados los mapas, no hay necesidad de estar conectado para ejecutar la simulación
- se puede usar un GPS externo para obtener la posición exacta de la estación. Aunque esto no es muy usado, puede ser útil a veces
- trabaja en Windows (también en Linux, pero no directamente)
- requiere de descargas grandes. Si su ancho de banda es limitado, descargar muchos mapas puede ser un problema. La versión online puede funcionar con descargas más pequeñas
- no es amigable, sobre todo para principiantes

La página principal de Radio Mobile, con ejemplos y tutoriales es:

http://www.cplus.org/rmw/english1.html

Siga las instrucciones para instalar el software en Windows.

Radio Mobile en línea

Para usar la versión en línea de Radio Mobile debe, en primer lugar crear una cuenta.
Vaya a: http://www.cplus.org/rmw/rmonline.html y cree la cuenta.

Usted va a recibir un correo de confirmación en pocos minutos y ya estará listo para empezar.
Para simular un enlace se necesita seguir ciertos pasos indicados en el menú de la izquierda, de arriba a abajo como se muestra en la figura PD 7 a continuación.

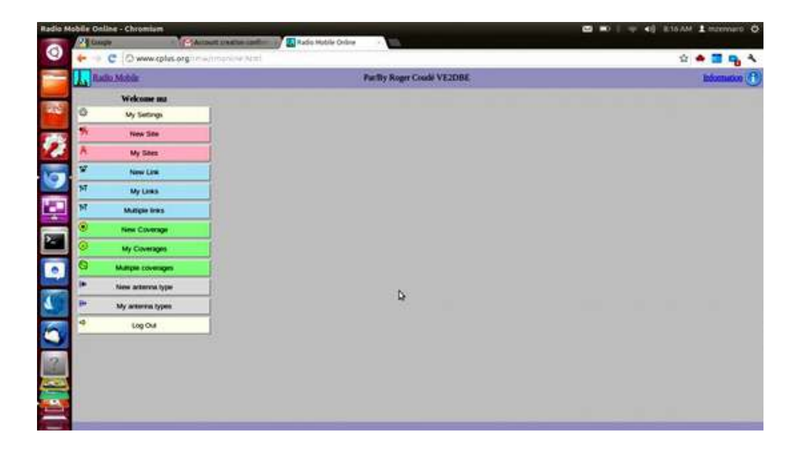


Figura PD 7: Preparación para simular un enlace usando Radio Mobile

El primer paso es hacer click en New Site. En seguida le presentarán un Mapa, similar a los Mapas Google. Puede hacer zoom en el mapa para encontrar la ubicación de su primer sitio. Arrastre el Marcador Naranja y colóquelo en la posición deseada. Cuando esté listo, haga click en Submit.

Déle un nombre apropiado a su ubicación y seleccione Add to my Sites. De esta manera, usted podrá usar esta ubicación para la simulación.
Repita el mismo proceso para el segundo sitio.

Una vez que tenga por lo menos dos sitios, puede seguir al próximo paso. La interfaz no le va a permitir registrar de una vez las coordenadas del sitio, así que se debe colocar el cursor en una posición aproximada para luego corregir el valor de las coordenadas en la tabla.
El segundo paso incluye registrar la información del enlace: características del equipo, de las antenas, etc.
Seleccione New Link en el menú de la izquierda. Seleccione ahora los dos sitios en los menús desplegables. La sensibilidad del receptor está expresada en microvoltios, mientras que normalmente usamos dBm.

Para convertir microvoltios a dBm le damos algunos ejemplos:

-90 dBm son 7.07 microvoltios
-85 dBm son 12.6 microvoltios
-80 dBm son 22.4 microvoltios
-75 dBm son 39.8 microvoltios
-70 dBm son 70.7 microvoltios

Es muy importante escoger una frecuencia que Radio Mobile en línea pueda manejar.
A continuación damos las frecuencias más importantes para enlaces WiFi

Use 2 300 MHz para enlaces de 2.4 GHz y 5 825 MHz para enlaces de 5.8 GHz.

Cuando haya registrado toda la información, seleccione *Submit*. En poco tiempo le presentarán una figura parecida a la siguiente.

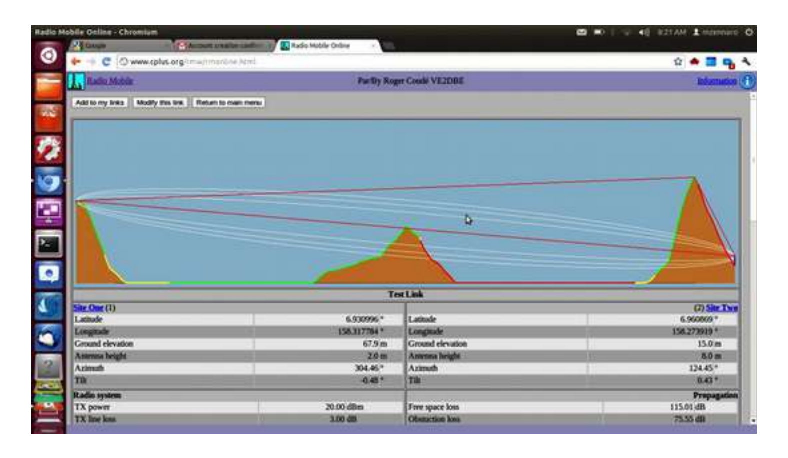


Figura PD 8: Resultado de la simulación

Esta página tiene toda la información necesaria para entender si el enlace es o no viable.
Le da información sobre: la longitud del enlace, el azimut, la elevación e inclinación que se debe dar a las antenas, la pérdida en espacio libre, la pérdida total en la trayectoria incluyendo la pérdida estadística y, lo más importante, el nivel de la señal recibida.

Con la sensibilidad del receptor que usted registró se le presentará el margen de desvanecimiento y será capaz de determinar si el enlace es posible o no. Si está satisfecho con los resultados, seleccione al comienzo de la página *Add to my sites* y el enlace va a ser guardado. Si no está satisfecho, y quiere hacer otra simulación con diferentes valores para el equipo, seleccione entonces *Modify this link*.

Radio Mobile para Windows en pasos sencillos

Presentamos una guía resumida para comenzar a usar Radio Mobile después de instalarlo. Los parámetros que no se especifican aquí pueden ser empleados en su valor por defecto y luego modificarlos en caso necesario.

Paso 1: descargue los mapas de la elevación digital (DEM) de su área de interés. Elija el formato SRTM.

Paso 2: crear un mapa. Vaya a "File" →"Map properties", escoja el punto medio de su área de interés como coordenadas de su mapa y un tamaño en km lo suficientemente grande como para incluir todo sus puntos. Use 514X514 pixeles por ahora. Puede añadir otro tipo de mapa (uno con carreteras, por ejemplo) al básico DEM si desea.

Paso 3: crear sistemas. Siga los pasos "File" →"Network properties" →"Systems". Cada uno es una combinación de potencia TX, sensibilidad RX y ganancia de antena. Seleccione antenas omni incluso si su antena es direccional, pero registre la ganancia real.

Paso 4: crear unidades. Cada unidad tiene un nombre y una posición geográfica. Puede usar grados, minutos, segundos, o grados y fracciones, pero asegúrese de elegir los hemisferios correctos (N, S, E u O).

Paso 5: asignar roles: seleccione "*Networks properties*" del menú "*File*". Luego vaya a la pestaña "*Membership*" donde podrá editar el sistema y el rol para cada unidad. Active cada unidad en la lista con una marca (√) . Asígnele un nombre a su red y en la pestaña "*Parameters*" fije las frecuencias mínimas y máximas de operación en MHz.

Paso 6: Vea su red en el mapa. Seleccione "View" →"Show networks"→"All"

Paso 7: Obtenga el perfil y el presupuesto del enlace punto a punto. “Tools” →”Radio link”. Puede cambiar a la vista detallada que le da una descripción textual del resultado de la simulación.

Paso 8: Vea la cobertura: Vaya a “Tools” → “Radio coverage” → “Single polar” para obtener la cobertura de cada estación. Aquí se hace relevante el tipo de antena. Si no es una omni, debería modificar el diseño de la antena y la orientación a la cual apunta la antena.

Cómo usar Google Earth para obtener un perfil de elevación

Google Earth es una aplicación para mapas muy popular. Puede usarse para obtener el perfil de elevación entre dos puntos y, por lo tanto, determinar si existe o no la línea de vista óptica.
La línea de vista radioeléctrica puede derivarse de la óptica sumando el efecto de la curvatura de la tierra (usando el radio modificado de la tierra) y los requisitos de despeje la primera zona de Fresnel.

El procedimiento es el siguiente:

Instale Google Earth en su dispositivo, abra la aplicación y haga zoom en el mapa de manera en que se puedan ver los dos puntos que quiere conectar.

1. En el menú superior seleccione “*Add path*”
2. Haga click para seleccionar el primer punto y lo mismo para el segundo
3. Déle un nombre a la conexión (“Enlace” por ejemplo) y seleccione OK en la ventana emergente
4. La conexión aparece en el menú de la izquierda
5. Haga click en el botón derecho en el nombre de la conexión (“Enlace” en nuestro ejemplo)
6. Seleccione “*Show elevation profile*”
7. El perfil de elevación va a aparecer al fondo de la pantalla.
8. Si se mueve en el perfil, va a ver una flecha roja que le muestra dónde está el punto en el mapa

Cómo evitar el ruido

Las bandas libres de licenciamiento ISM y U-NII representan una porción muy pequeña del espectro electromagnético conocido. Debido a que esta región puede ser utilizada sin pagar costos de licenciamiento, muchos dispositivos comerciales la utilizan para un amplio rango de aplicaciones.
Teléfonos inalámbricos, transmisores analógicos de video, *Bluetooth*, monitores de bebés, e incluso los hornos de microondas compiten con las redes de datos inalámbricas por el uso de la muy limitada banda de 2.4 Ghz. Esas señales, así como las de otras redes inalámbricas locales, pueden causar problemas significativos para los enlaces inalámbricos de largo alcance. Para reducir la recepción de señales no deseadas le describimos algunos pasos que puede utilizar.

Incremente la ganancia de la antena en ambos extremos del enlace punto a punto. Las antenas no sólo agregan ganancia a un enlace, sino que el aumento de la directividad tiende a rechazar el ruido proveniente de los alrededores del enlace. Dos antenas de alta ganancia que estén enfocadas entre sí, rechazarán el ruido que esté fuera de la trayectoria del enlace. Si utilizamos antenas omnidireccionales recibiremos ruido de todas las direcciones.

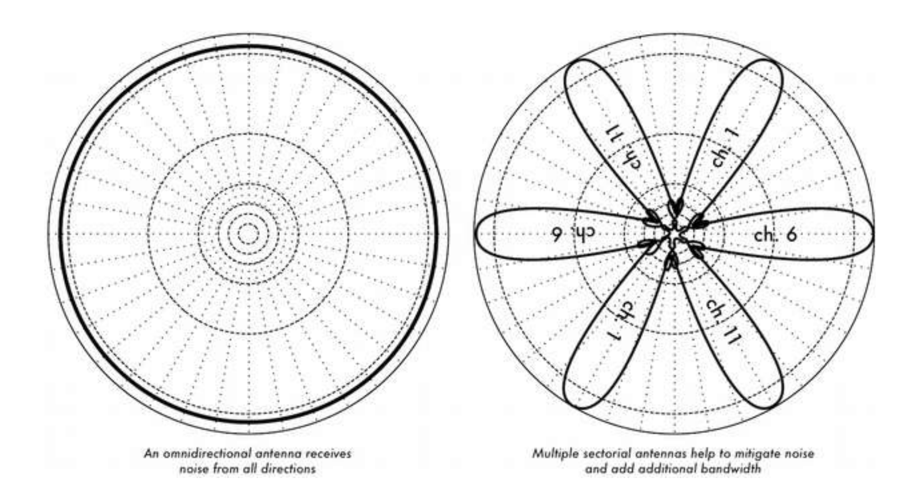


Figura PD 9: Una sola antena omnidireccional versus múltiples antenas sectoriales

Utilice antenas sectoriales en lugar de omnidireccionales. Haciendo uso de varias antenas sectoriales puede reducir el ruido global recibido en un punto de distribución. Si traslapa los canales utilizados en cada antena sectorial, también puede incrementar el ancho de banda disponible para sus clientes.

No utilice un amplificador. Los amplificadores pueden hacer que los problemas de interferencia empeoren con la amplificación indiscriminada de todas las señales recibidas, incluyendo las fuentes de interferencia. Los amplificadores también causan problemas de interferencia para los otros usuarios de la banda que se encuentren cerca.

Utilice el mejor canal disponible. Recuerde que los canales 802.11b/g tienen un ancho de 22 MHz, pero están separados sólo por 5 MHz.
Realice una prospección del sitio, y seleccione el canal que esté tan lejos como sea posible de las fuentes de interferencia existentes. Tenga en cuenta que el paisaje inalámbrico puede cambiar en cualquier momento ya que la gente puede agregar nuevos dispositivos (teléfonos inalámbricos, otras redes, etc.). Si de repente su enlace presenta problemas para enviar paquetes es posible que deba realizar otra prospección y escoger un canal diferente.

Si es posible, utilice las bandas de 5.8 G Hz. Si bien esta es sólo una solución a corto plazo, actualmente la mayor parte del equipo instalado utiliza 2.4 GHz. Utilizar 802.11a, le va a permitir eludir esta congestión.

Si todo esto falla, utilice un espectro con licenciamiento. Hay lugares donde todo el espectro sin licenciamiento está ocupado. En esos casos, puede tener sentido gastar el dinero adicional para obtener la licencia respectiva e instalar un equipo que utilice una banda menos congestionada. Para enlaces punto a punto de larga distancia que requieren de muy alto rendimiento y máximo tiempo de disponibilidad, esta es ciertamente una opción. Por supuesto esto implica un precio mucho mayor comparado con el equipo sin licenciamiento.
Recientemente, hay equipos disponibles en las bandas de 17 y 24 GHz.
A pesar de que es bastante más caro, ofrece mayor ancho de banda y en muchos países estas frecuencias no requieren licencia.
Para identificar las fuentes del ruido, necesita herramientas que le muestren qué está sucediendo en el aire a 2.4 GHz. Vamos a ver algunos ejemplos de estas herramientas en los capítulos **Monitoreo de la Red** y **Mantenimiento y Solución de Problemas.**

Repetidores

El componente más crítico para construir un enlace de red a larga distancia es la existencia de ***línea visual*** (a menudo abreviada como ***LOS*** por su sigla en inglés –*Line of Sight*).
Los sistemas de microondas terrestres simplemente no pueden tolerar colinas altas, árboles, u otros obstáculos en el camino de un enlace a larga distancia. Es necesario que se tenga una idea del relieve de la tierra entre dos puntos antes de poder determinar si un enlace es posible.
Pero aún si hay una montaña entre dos puntos, debemos tener presente que los obstáculos pueden ser transformados en ventajas.
Las montañas pueden bloquear la señal, pero suponiendo que se pueda proveer energía, también pueden actuar como muy buenos puntos repetidores.
Los repetidores son nodos que están configurados para transmitir el tráfico no destinado al nodo mismo. En una red en malla, cada nodo es un repetidor.
En una red de infraestructura tradicional, los nodos repetidores deben ser configurados específicamente para poder pasar el tráfico a otros nodos.
Un repetidor puede usar uno o más dispositivos inalámbricos.
Cuando utiliza un sólo radio (denominado repetidor de un solo brazo), el caudal global es ligeramente menor que la mitad del ancho de banda disponible, puesto que el radio puede enviar o recibir datos, pero no simultáneamente. Esos dispositivos son baratos, simples y tienen bajo consumo de potencia. Un repetidor con dos (o más) tarjetas de radio puede operar todos los radios a toda capacidad, siempre que los mismos estén configurados para usar canales que no se superpongan. Por supuesto, los repetidores también pueden proveer una conexión Ethernet para conectividad local.
Los repetidores pueden adquirirse como un juego completo, o fácilmente ensamblados conectando dos o más nodos inalámbricos con un cable Ethernet.
Cuando planee usar un repetidor construido con tecnología 802.11, tenga en cuenta que cada nodo debe ser configurado en el modo máster, administrado o *ad-hoc* que le corresponda.
Generalmente, ambos radios en el repetidor están configurados en el modo máster para permitir que los múltiples clientes puedan conectarse a cualquier lado del repetidor. Pero dependiendo de su diseño de red, uno o más dispositivos van a necesitar utilizar el modo *ad-hoc*, o el modo cliente.

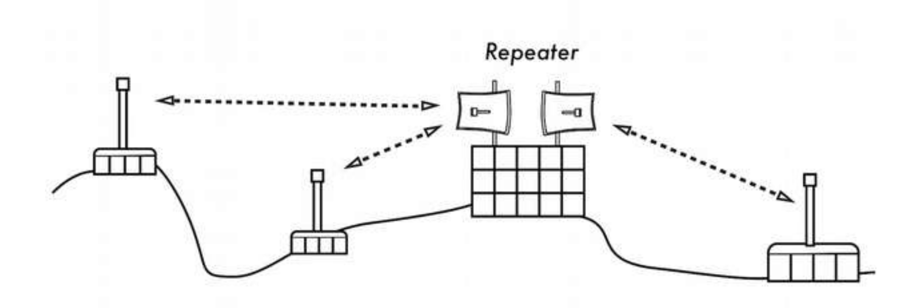


Figura PD 10: El repetidor remite los paquetes por el aire entre los nodos que no tienen línea visual directa

En general, los repetidores son utilizados para evitar obstáculos en el camino de un enlace a larga distancia, como edificios en la trayectoria; pero esos edificios contienen gente. A menudo podemos hacer acuerdos con los dueños de los edificios para proporcionarles ancho de banda a cambio de utilizar el techo y la electricidad. Si el dueño del edificio no está interesado, podemos intentar persuadir a los inquilinos de los pisos más altos para instalar equipos en una ventana.
Si usted no puede pasar sobre o a través de un obstáculo, a menudo lo puede rodear. En lugar de usar un enlace directo, intente hacer trayectos múltiples para eludir el obstáculo.

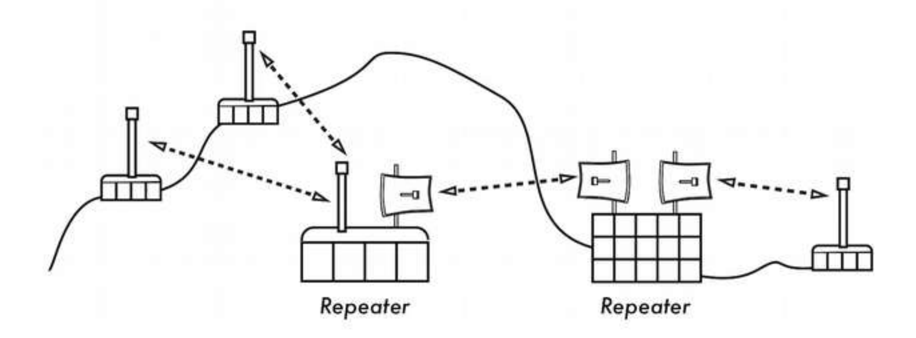


Figura PD 11: No había energía disponible en lo alto de la colina, pero esto fue eludido con el uso de múltiples repetidores ubicados alrededor de la base

Finalmente, usted podría necesitar retroceder para poder avanzar. Si tenemos un lugar alto en una dirección diferente, y ese lugar puede ver más allá del obstáculo, se puede hacer un enlace estable a través de una ruta indirecta.

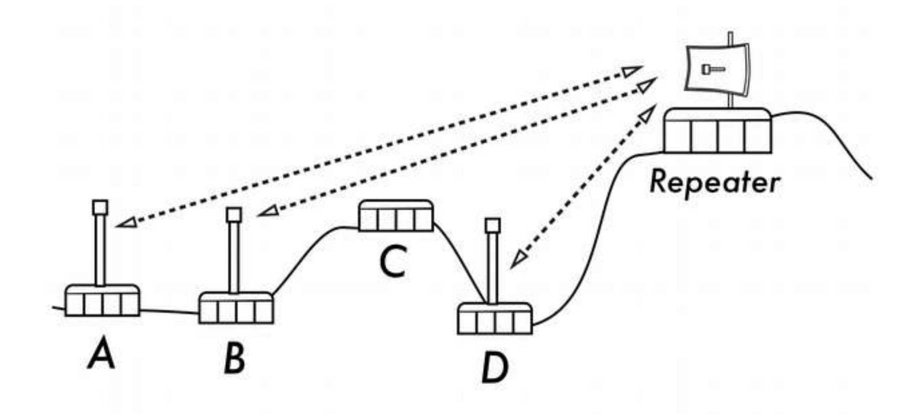


Figura PD 12: El sitio D no puede establecer un buen enlace con A o B, porque C está obstruyendo y no alberga un nodo. Al instalar un repetidor en un lugar alto, los nodos A, B, y D se pueden comunicar. El tráfico desde el nodo D en realidad viaja más lejos que el del resto de la red antes de que el repetidor reenvíe esos datos

Planificación de despliegues en IPv6

Como ya mencionamos en el capítulo **Redes**, todas las regiones del mundo han agotado sus direcciones IPv4.
Por ello es importante que usted incorpore en sus planes la instalación de redes basadas en IPv6.

Para el momento de la escritura de este libro habrá muchos sitios y servicios solamente disponibles en IPv4.
Así que para convertirse en un líder de instalaciones en IPv6, usted va a necesitar interactuar con las redes IPv4 todavía en existencia, y al mismo tiempo enseñar y guiar a sus usuarios y desarrolladores en el manejo de IPv6 al mismo tiempo que de IPv4.

Al convertirse en pionero de las instalaciones en IPv6 en su red, estará a la vanguardia de Internet y será reconocido como alguien preparado en el conocimiento y respaldo de la próxima generación de las redes informáticas.

En su preparación para Ipv6 le damos algunos pasos a seguir para avanzar en la dirección adecuada:

1. No compre enrutadores, firewalls (cortafuegos) u otro equipo IP que procese paquetes IPv4 en el hardware a toda velocidad y que solo procese paquetes en IPv6 más lentamente, en software; o peor aún, que todavía no maneje IPv6. La gran mayoría de los dispositivos disponibles admiten IPv6. RIPE (Réseaux IP Européens ha preparado algunos requisitos para incluir en cualquier licitación a manera de garantizar que IPv6 se incluya: http://www.ripe.net/ripe/docs/current -ripe-documents/ripe-554 También puede buscar el logo IPv6-Ready en la hoja de datos de los dispositivos.
2. Cuando instale software nuevo, asegúrese de que trabaje en IPv6.
3. Cuando discuta sobre el enlace con el proveedor de servicio (ISP) local, asegúrese de que hayan instalado o tengan planes de instalar y ofrecer servicios IPv6. De lo contrario, discuta cómo puede usted colaborar e interconectar su red IPv6 con ellos. El costo de IPv6 debe incluirse en el precio general; esto significa que no debe hacer un pago adicional para tener IPv6. El Acuerdo de Nivel de Servicio (Service Level Agreement: SLA) para IPv6 debe ser idéntico al de IPv4 (caudal, latencia, tiempo de respuesta incidente, etc.). Hay varias técnicas de transición IPv4/IPv6 que pueden desplegarse.

Las siguientes direcciones pueden darle información actualizada al respecto:
http://www.petri.co.il/ipv6-transition.htm
http://en.wikipedia.org/wiki/IPv6_transition_mechanisms
http://www.6diss.org/tutorials/transitioning.pdf

Hay más información sobre el crecimiento de IPv6 y la carencia de direcciones disponibles IPv4 en el siguiente artículo publicado a fines del 2012:
http://arstechnica.com/business/2013/01/ipv6-takes-one-step-forward-ipv4-two-steps-back-in-2012/

También hubo un proyecto financiado por la CE (Comunidad Europea) llamado 6Deploy que ofrecía entrenamiento y asistencia técnica para ingenieros de redes que estaban comenzando sus instalaciones en IPv6:
http://www.6deploy.eu/index.php?page=home

11. SELECCIÓN Y CONFIGURACIÓN DEL HARDWARE

En los últimos años, el surgimiento de un interés sin precedentes en el equipamiento para redes inalámbricas ha traído una enorme variedad de equipos de bajo costo al mercado. Tanta variedad, que resultaría imposible catalogar cada uno de los componentes disponibles. En este capítulo, nos enfocamos en señalar la clase de características y atributos que son deseables en los componentes inalámbricos.

Cableado inalámbrico

Con un nombre como el de "inalámbrico", usted podría sorprenderse de cuántos cables están involucrados en el desarrollo de un simple enlace punto a punto.

Un nodo inalámbrico está conformado por varios componentes que deben estar conectados entre sí con el cableado apropiado. Obviamente, se necesita al menos una computadora conectada a una red Ethernet, y un enrutador inalámbrico, o un puente en la misma red. Los componentes de radio deben conectarse a las antenas, pero en el trayecto pueden necesitar conectarse con un protector contra rayos u otro dispositivo. Muchos de éstos requieren energía, ya sea a través de otro cable AC, o utilizando un transformador DC. Todos estos componentes utilizan varias clases de conectores, sin mencionar una amplia variedad de tipos de cable de diferentes calibres.

Ahora multiplique esos cables y conectores por el número de nodos que va a instalar, y bien puede estar preguntándose porqué nos referimos a esta tecnología como sin cables o "inalámbrica".

El diagrama en la siguiente página le va a dar alguna idea del cableado necesario para un enlace típico punto a punto.

Note que este diagrama no está a escala y no es necesariamente la mejor opción para el diseño de su red, pero le permitirá conocer en principio la variedad de conectores y componentes comunes que probablemente encontrará en el mundo real.

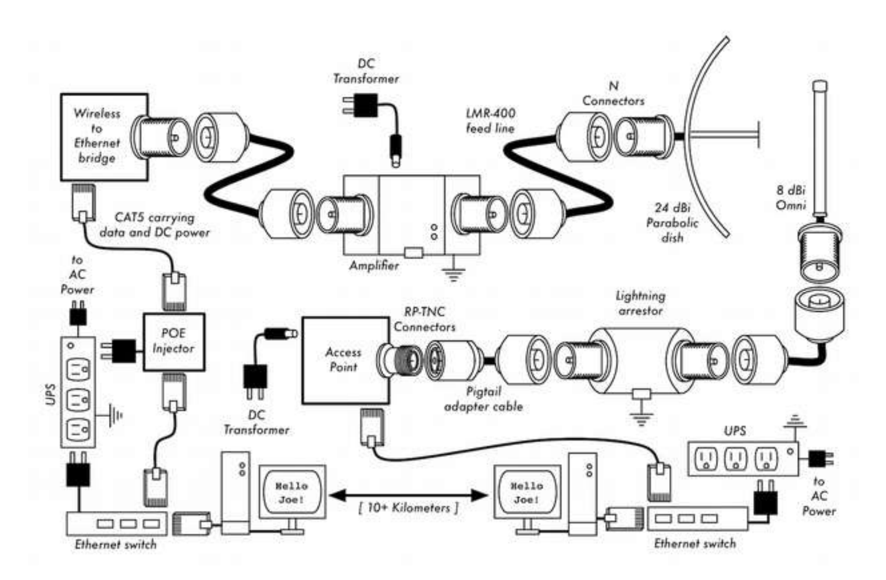


Figura SCH1: Interconexiones y componentes comunes de un enlace inalámbrico Punto a Punto

Aunque los componentes utilizados varían de nodo a nodo, toda instalación va incorporar estas partes:

1. Una computadora o una red conectada a un conmutador Ethernet.
2. Un dispositivo que conecte esa red a un dispositivo inalámbrico (un enrutador inalámbrico, un puente o un repetidor).
3. Una antena, integrada en el dispositivo inalámbrico, o conectada mediante un cable apropiado.
4. Componentes eléctricos constituidos por fuentes de alimentación, acondicionadores de energía, y protectores contra rayos.

La selección del equipo debe determinarse estableciendo las exigencias del proyecto, el presupuesto disponible, y verificando que el proyecto sea viable utilizando los recursos disponibles (incluyendo previsiones para repuestos y costos de mantenimiento). Como discutimos en otros capítulos, establecer el alcance de su proyecto es básico antes de tomar cualquier decisión de adquisiciones.

Cómo elegir los componentes inalámbricos

Desafortunadamente, en un mundo de fabricantes de equipo que compiten entre sí y con una disponibilidad limitada de fondos, el tema del precio es el factor que generalmente recibe la mayor atención. El viejo dicho "tanto pagas, tanto obtienes" se cumple cuando compramos equipos de alta tecnología, pero no debe ser considerado como una verdad absoluta. Mientras que el precio es una parte importante de cualquier decisión de compra, es de vital importancia comprender precisamente qué es lo que puede obtener por su dinero, para que pueda hacer una elección que se ajuste a sus necesidades. Cuando compare equipos inalámbrico para usar en su red, asegúrese de considerar estas variables:

Interoperabilidad. ¿El equipamiento que está considerando funcionará con el de otros fabricantes? Si no es así, ¿es un factor importante para este segmento de su red? Si el equipo en cuestión acepta un estándar (como el 802.11b/g), entonces probablemente va a funcionar con el proveniente de otras fuentes.

Alcance. No es algo inherente a una pieza particular del equipo. El alcance de un dispositivo depende de la antena conectada a él, el terreno que lo rodea, y las características del dispositivo en el otro extremo del enlace, y otros factores. En lugar de confiar en el valor semi-ficticio del "alcance" presentado por el fabricante, es más útil conocer la ***potencia de transmisión*** del radio así como la ***ganancia de la antena*** (si está incluida la antena). Con esta información usted puede calcular el alcance teórico como se hace al calcular el presupuesto del enlace descrito en el capítulo **Planificar la Instalación.**

Sensibilidad del radio. ¿Cuán sensible es el dispositivo de radio a una tasa de transferencia dada? El fabricante debe proveer esta información, al menos a las velocidades más rápidas y más lentas. Esto puede utilizarse como una medida de la calidad del equipo, y le permite completar el cálculo del presupuesto del enlace. Recuerde que mientras más bajo sea este valor mejor será la sensibilidad del radio.

Caudal (t*hroughput*). Los fabricantes sistemáticamente ponen la tasa de transferencia más alta posible como la "velocidad" de su equipo. Tenga en mente que el valor de la tasa de transferencia del radio (ej. 54 Mbps) nunca es el verdadero caudal neto del dispositivo (ej. aproximadamente 22 Mbps para 802.11g).

Si la información del caudal neto no está disponible para el dispositivo que usted está evaluando, un buen truco es dividir la "velocidad" del dispositivo entre dos, y restar el 20%, más o menos. Si tiene alguna duda, realice la prueba de caudal neto en una unidad de evaluación antes de comprometerse a adquirir una gran cantidad de equipos que no especifican una tasa oficial de caudal neto.

Accesorios necesarios. Para mantener el precio inicial bajo, los vendedores a menudo quitan accesorios que se requieren para un uso normal. ¿El precio incluye todos los adaptadores de energía? (Las fuentes DC generalmente se incluyen; pero los inyectores de potencia para Ethernet (*Power Over Ethernet*) en general no. Del mismo modo, revise dos veces los voltajes de entrada, ya que el equipo normalmente viene con especificaciones de alimentación correspondiente a los estándares utilizados en los EEUU. ¿Viene con los latiguillos (*pigtails*), adaptadores, cables, antenas, y las tarjetas de radio? Si piensa usarlo en exteriores, ¿incluye el dispositivo una caja impermeable?

Disponibilidad. ¿Va a ser capaz de reemplazar los componentes que se rompan? ¿Puede ordenar esa pieza en grandes cantidades en caso de que su proyecto lo necesite? ¿Cuál es el lapso de vida proyectado de este producto en particular, tanto en términos de tiempo de funcionamiento en el campo y de la probabilidad de que el vendedor lo siga suministrando?

Consumo de energía. Para instalaciones remotas el consumo de energía es el detalle más importante. Si los dispositivos van a ser alimentados con paneles solares es muy importante escoger los que necesiten la más baja energía. El costo de paneles solares y baterías puede ser más elevado que el de los dispositivos inalámbricos; por lo tanto, un consumo bajo de energía va a redundar en un presupuesto general más bajo.

Otros factores. Asegúrese de que se especifiquen otros detalles importantes para satisfacer sus necesidades particulares. Por ejemplo, ¿incluye el dispositivo un conector para una antena externa? Si lo incluye, ¿de qué tipo es? ¿Existen limitaciones en número de usuarios o en el caudal impuestas por software, y si las hay, cuál es el costo de extender esos límites? ¿Cuál es la forma física del dispositivo? ¿Cuánta potencia consume? ¿Soporta POE como fuente de potencia?

¿Provee encriptación, NAT, herramientas de monitoreo de ancho de banda, u otras características críticas para el diseño de la red planeada?

Contestando estas preguntas primero, usted va a poder tomar decisiones de compra inteligentes cuando sea el momento de elegir el equipamiento de la red. Es casi imposible poder resolver todas las dudas antes de comprar el equipo, pero si le da prioridad a estas preguntas y presiona al vendedor para que las conteste antes de comprometerse a comprar, hará un mejor uso de su presupuesto y va a construir una red con componentes adecuados a sus necesidades.

¿Soluciones comerciales o Soluciones DIY?

Lo más seguro es que su proyecto de red incluya componentes adquiridos a través de proveedores externos, así como otros conseguidos o fabricados localmente. Esta es una verdad económica en la mayor parte del mundo. En este estadio de la tecnología humana, la distribución global de la información es algo sencillo en comparación con la distribución global de bienes. En muchas regiones, importar cada componente necesario para construir la red es excesivamente caro para la mayoría de los presupuestos, excepto para los muy grandes. Se puede ahorrar mucho dinero a corto plazo encontrando fuentes locales para partes y mano de obra, e importar sólo aquellos componentes que lo ameriten.

Por supuesto que hay un límite a lo que puede hacer una persona o un grupo en un tiempo determinado. Para ponerlo de otra forma, mediante la importación de tecnología, se intercambia dinero por equipamiento que le puede solucionar un problema particular en un periodo comparativamente inferior de tiempo. El arte de construir infraestructuras de comunicaciones locales está en encontrar el correcto balance entre el dinero y el esfuerzo que se necesita para resolver un problema dado.

Algunos componentes como las tarjetas de radio y los cables de antenas, son definitivamente muy complejos como para considerar fabricarlos localmente. Sin embargo, otros elementos como las antenas y las torres son relativamente simples y pueden hacerse a nivel local por una fracción del costo de importación.

Entre estos dos extremos se encuentran los dispositivos de comunicación en sí.

Utilizando componentes disponibles como las tarjetas de radio, placas madre, y otros, se pueden construir dispositivos con características comparables (o incluso superiores) a la mayoría de las implementaciones comerciales. Combinar plataformas de hardware abiertas con software de fuente abierta puede resultar en una verdadera ganga, porque ofrece soluciones robustas y a la medida por muy bajo costo.

Esto no implica que el equipamiento comercial sea inferior a una solución "hágalo usted mismo". Al ofrecernos las conocidas "llave en mano", los fabricantes no sólo nos ahorran tiempo de desarrollo, sino que también permiten que una persona relativamente poco calificada puedan instalar y mantener el equipamiento. La fortaleza principal de las soluciones comerciales es que ellas proveen **soporte** y **garantía de los equipos** (usualmente limitada). También tienen una **plataforma consistente** que hace que las instalaciones de red sean muy estables y a menudo intercambiables.

Si una parte del equipamiento no funciona, es difícil de configurar, o tiene problemas, un buen fabricante lo va a asistir. Si en uso normal el equipo falla (excluyendo daños extremos, como los ocasionados por la caída de un rayo), el fabricante lo va a reemplazar. La mayoría ofrecen esos servicios por un tiempo limitado como parte del precio de compra, y otros brindan soporte y garantía por un período de tiempo extendido mediante el pago de una cuota mensual. Teniendo una plataforma consistente es sencillo tener los repuestos a mano y simplemente sustituir el equipo que falla sin la necesidad de un técnico que lo configure. Evidentemente esto viene de la mano de un costo inicial más alto si lo comparamos con los componentes disponibles localmente.

Desde el punto de vista de un arquitecto de red, los tres grandes riesgos ocultos al elegir soluciones comerciales son: ***quedar atrapado con un proveedor***, las ***líneas de productos descontinuadas***, y ***los costos de licenciamiento futuro***.

Puede ser muy costoso dejar que las nuevas "prestaciones" mal definidas dirijan el desarrollo de su red. Los fabricantes frecuentemente van a ofrecerle prestaciones que son incompatibles por su diseño con los de la competencia, y luego usan elementos de mercadeo para convencerlo de que usted no puede vivir sin éstas, sin importar que la prestación contribuya o no a solucionar sus problemas de comunicación.

Al empezar a contar con esas prestaciones, probablemente en el futuro decidirá continuar comprando los equipos del mismo fabricante.

Esa es la definición de “quedar atrapado” con el proveedor. Si una gran institución utiliza una cantidad significante de equipo patentado, es improbable que simplemente lo abandone para considerar un proveedor diferente. Los expertos en ventas saben esto (y de hecho, algunos cuentan con ello) y lo utilizan como estrategia para la negociación de precios.

Un fabricante puede eventualmente decidir descontinuar una línea de productos sin importar su popularidad. Esto asegura que los clientes, que ya confiaban en las características del producto patentado del fabricante, van a comprar los nuevos modelos (casi siempre más caros). Los efectos a largo plazo de quedar atrapado con el proveedor y con los productos descontinuados son difíciles de estimar cuando planificamos un proyecto de red, pero deben tenerse en cuenta.

Finalmente, si una pieza en particular del equipamiento utiliza un código de computadora patentado, usted va a tener que licenciar el uso de ese código en contratos futuros. El costo de esas licencias puede variar dependiendo de las características que brinda, el número de usuarios, la velocidad de la conexión u otros factores. Si no se paga el costo de la licencia, algunos equipos están diseñados para !simplemente dejar de funcionar hasta que se provea una licencia válida! Asegúrese de comprender las cláusulas de uso de cualquier equipamiento que adquiera, incluyendo las futuras cuotas de licenciamiento.

Usando equipamiento genérico que respalda estándares abiertos y software de fuente abierta, se pueden evitar algunos de estos riesgos. Por ejemplo, es muy difícil verse atrapado por un proveedor que utiliza protocolos abiertos (tales como TCP/IP sobre 802.11a/b/g). Si tiene un problema con el equipo o con el proveedor, siempre puede adquirirlo de otro proveedor, ya que va a funcionar con lo que usted ya compró. Es por estas razones que recomendamos utilizar protocolos patentados y espectro con licenciamiento **sólo** cuando el equivalente abierto (como el 802.11a/b/g) no sea viable técnicamente.

Asimismo, los productos individuales pueden descontinuarse en cualquier momento, pero usted puede limitar el impacto que esto va a tener en su red utilizando componentes genéricos. Por ejemplo, si una *placa madre* particular ya no está disponible en el mercado, puede tener a mano varias *placas madre* de PC que realicen efectivamente la misma tarea.

Más adelante en este capítulo vamos a ver algunos ejemplos de cómo utilizar esos componentes genéricos para construir un nodo inalámbrico completo.

Obviamente, no va a haber costos de licenciamiento en cuanto al software libre (con la excepción de un proveedor que ofrezca soporte u otros servicios sin cobrar por el uso del software en sí mismo).

Ha habido ocasionalmente vendedores que se aprovechan indebidamente del regalo que los programadores de fuente abierta le han dado al mundo, exigiendo el pago de licencias, en violación flagrante de las cláusulas de distribución establecidas por los autores originales. Sería bueno evitar a dichos vendedores, y desconfiar de aquellas afirmaciones de "software libre" que estipulan una cuota de licenciamiento futuro. La desventaja de utilizar software libre y equipamiento genérico es claramente una cuestión de soporte.

Cuando lleguen los problemas a la red, va a tener que resolverlos por usted mismo. Esto a veces se logra consultando recursos gratuitos en línea y motores de búsqueda, y aplicando los parches al código directamente.

Si no tiene ningún miembro de su equipo que sea competente en el tema y se dedique a diseñar soluciones a sus problemas de comunicación, entonces poner en marcha un proyecto de red puede tomar una cantidad considerable de tiempo. Por supuesto que tampoco hay garantías de que simplemente "a punta de dinero" se resuelva el problema. Si bien damos varios ejemplos de cómo hacer el trabajo usted mismo/a, seguramente le va a resultar un gran desafío. Necesita encontrar el balance entre el enfoque de las soluciones comerciales y las hechas por usted mismo/a, que funcionen de forma adecuada a su proyecto.

En resumen, siempre defina primero el objetivo de su red, identifique los recursos que puede tener para lidiar con el problema, y permita que la selección del equipamiento emerja naturalmente de esos resultados. Considere las soluciones comerciales así como los componentes abiertos, manteniendo siempre en mente los costos a largo plazo de ambas.

Cuando considere cuál es el equipamiento que va a usar recuerde siempre comparar la distancia útil esperada, confiabilidad y caudal neto (throughput), además del precio. Asegúrese de incluir cualquier cuota de licenciamiento futuro cuando calcule el costo total del equipamiento.

Finalmente, compruebe que los radios que va a comprar operan en una banda exenta de licencia donde los va a instalar; o, si debe usar espectro sujeto a licencia, que se cuenta con los recursos y los permisos para pagar las licencias requeridas.

Protección profesional contra rayos

Los rayos son el predador natural de los equipos inalámbricos. A continuación vemos un mapa que muestra la distribución global de los rayos entre 1995 y 2003.

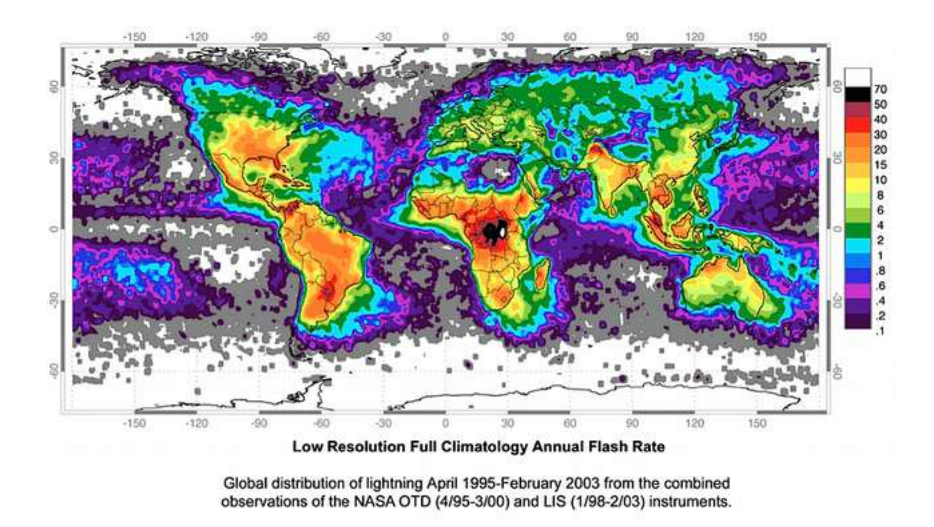


Figura SCH 2: Distribución global de rayos desde 1995 a 2003

Hay dos formas diferentes mediante las cuales un rayo puede dañar el equipo: con un impacto directo o por inducción. Los impactos directos ocurren cuando el rayo realmente alcanza la torre o la antena. El impacto inducido se produce cuando el rayo cae cerca de la torre.

Imagine la descarga de un rayo cargado negativamente. Como las cargas iguales se repelen entre sí, esto ocasiona que los electrones en el cable se alejen del rayo, creando corriente en las líneas. Esta corriente podría ser mucho mayor que la que el receptor de radio puede manejar. En general, cualquier tipo de rayo va a destruir el equipo que esté sin protección.



Figura SCH3: Torre con un cable de cobre grueso conectado a tierra

Proteger las redes inalámbricas de los rayos no es una ciencia exacta, y no hay garantías de que no vaya a caer un rayo, aún si se toman todas las precauciones. Muchos de los métodos utilizados ayudan a prevenir los impactos directos y los generados por inducción. Si bien no es necesario utilizar todos los métodos de protección contra rayos, tener más de uno va a ayudarnos a cuidar mejor el equipo. La cantidad de rayos observados históricamente en un área de servicio es la mejor guía para saber qué debemos hacer.
Comience en la base misma de la torre. Recuerde que la base de la torre está bajo tierra. Después de colocados los cimientos de la torre, pero antes de que el pozo se llene nuevamente, se debe instalar un aro de alambre trenzado grueso para hacer tierra, extendido bajo la superficie y sobresaliendo de la misma cerca de una de las patas de la torre.

El alambre debe ser por lo menos AWG #4 (diámetro *mayor de 5,19 mm*) o más grueso.

Adicionalmente, se debe enterrar una jabalina, y conectarla también a la torre en el mismo punto.

Es importante tener en cuenta que no todos los metales conducen la electricidad de la misma forma. Algunos metales actúan como conductores eléctricos mejor que otros, y las diferentes capas existentes en la superficie también pueden afectar cómo el metal de la torre maneja la corriente eléctrica. El acero inoxidable es uno de los peores conductores, y las capas contra la herrumbre como los galvanizados o la pintura reducen la conductividad del metal. Por esta razón se coloca un alambre de tierra trenzado desde la base de la torre hasta la cima. La base necesita estar apropiadamente unida a los conductores provenientes del aro y de la jabalina. La cima de la torre debe tener una jabalina pararrayos, terminada en punta. Cuanto más fina y aguda sea la punta, más efectivo será el pararrayos. El alambre de tierra trenzado desde la base tiene que terminarse en esta jabalina. Es muy importante asegurarse de que el alambre de tierra esté conectado al propio metal. Cualquier tipo de capa, como la pintura, debe removerse antes de conectar el alambre. Una vez que se hizo la conexión, si es necesario, el área expuesta puede repintarse, cubriendo el alambre y los conectores para proteger a la torre de la herrumbre y la corrosión.

La solución anterior detalla la instalación de un sistema básico de tierra. El mismo provee protección para la torre contra los impactos directos, y representa el sistema de base al que se conectará todo lo demás.

La protección ideal para los impactos indirectos son los protectores contra rayos de gas ubicados en ambos extremos del cable. Estos protectores deben conectarse directamente al alambre de tierra instalado en la torre si este está en el extremo más alto. El extremo en la base debe también conectarse a una buena tierra, como una placa de tierra o una tubería metálica que esté llena de agua. Es importante asegurarse de que el protector contra rayos externo esté impermeabilizado.

Muchos protectores contra rayos para los cables coaxiales son impermeables, mientras que los de cable CAT5 no lo son. En el caso de que no se usen los protectores contra rayos, y el cableado esté basado en coaxiales, se conecta el revestimiento del cable coaxial al cable de tierra instalado en las torres, y de esta forma habrá algo de protección. Esto proporciona un camino a tierra a las corrientes inducidas, y si la descarga no es muy fuerte no va a afectar el cable coaxial. Si bien este método no da una protección tan buena como la utilización de los protectores de gas, es mejor que nada.

Configuración del Punto de Acceso

En esta sección se presentará un procedimiento sencillo para la configuración básica de Puntos de Acceso y Clientes inalámbricos por medio de la revisión de sus componentes principales y el análisis de sus efectos en el comportamiento de la red.
Se darán también algunos trucos prácticos y orientación para resolver problemas.

Antes de comenzar

Cuando reciba un equipo inalámbrico nuevo tómese el tiempo necesario para familiarizarse con sus características principales; y asegúrese de:

- Descargar u obtener de alguna manera todos los **manuales de usuario** y **hojas de especificaciones** de los dispositivos que va a instalar.
- Si va a usar dispositivos de segunda mano, asegúrese de obtener la información completa sobre las configuraciones actuales o sobres las últimas conocidas, por ejemplo contraseñas, direcciones IP, etc.
- Tener diseñado un plan de la red que va a instalar que incluya **presupuesto de red**, **topología de la red**, **configuración** de **canales** y de **IP**.
- Tomar notas escritas de todas las configuraciones que va a utilizar, especialmente !de las **contraseñas**!
- Respaldar los archivos de la **última configuración que nos funcionó**.

Familiarizarse con el dispositivo

Como primer paso, es importante que conozca el significado de todos los LED de su aparato. La siguiente figura nos muestra el frente de un Punto de Acceso típico con varios LED encendidos.



Figura SCH 4: El frente de un Punto de Acceso (Access Point) típico

Los LED normalmente indican:

- Existencia de energía
- Puertos activos / tráfico (colores amarillo/verde)
- Estatus de error (color rojo)
- Intensidad de la señal recibida (barras de LED, algunas veces multicolores; algunos dispositivos, como *Ubiquiti* pueden ajustarse para encender cada LED para umbrales específico.

A veces hay diferentes significados asociados con el mismo LED pero usando colores o actividades diferentes (por ejemplo un LED prendido, apagado o destellante a velocidades diferentes).
Usted debería también identificar los diferentes puertos e interfaces:

- Interfaces de radio, a veces llamadas WLAN. Estas deberían tener una o más conectores de antenas (o antenas no despegables).
- Una o más interfaces Ethernet:
- Uno o más puertos para redes locales (LAN)
- Un puerto para conexión a Internet (llamado WAN)
- Entrada de alimentación (5, 6, 7.5, 12V u otros, normalmente corriente continua). Es realmente importante que la fuente de alimentación sea la adecuada para el voltaje. A veces, se proporciona la alimentación al dispositivo a través del mismo cable UTP que transporta los datos Ethernet. Esto se conoce como Power-over-Ethernet (PoE).
- Botón de encendido (no siempre hay uno).
- Botón de reinicio (*reset*) (a menudo "escondido" en un hueco pequeño; puede presionarse usando un clip de papel extendido).

El botón de reinicio puede tener efectos diferentes (desde un reinicio simple a un reinicio total a condiciones de fábrica) si se oprime brevemente o por un tiempo largo. Puede tomar 30 segundos o más para activar un reinicio total.
NOTA: hacer un *reset* total de un dispositivo (es decir, volver a las condiciones de fábrica) cuyo estado *desconocemos*, puede ser una tarea ingrata. Asegúrese de guardar por escrito la información sobre los parámetros críticos del dispositivo, como la dirección IP, y la máscara de red; también el nombre de usuario del administrador y su contraseña.

En la figura siguiente se muestra un Punto de Acceso Linksys corriente con el botón de encendido, los puertos, el botón de *reset* y dos antenas.

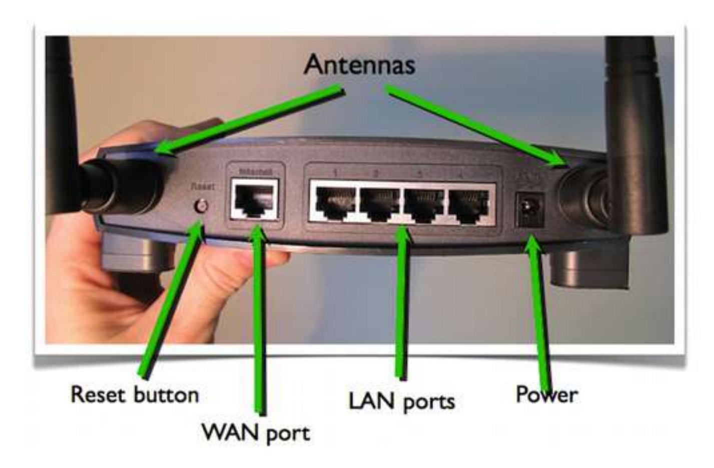


Figura SCH 5: Punto de Acceso (Access Point) Linksys

Interfaces de usuario

Se puede interactuar (i.e. dar instrucciones y cambiar configuraciones) con el Punto de Acceso de varias maneras dependiendo del tipo de hardware que se esté usando. Estas maneras son las siguientes:

- Interfaz Gráfica de Usuario (página web)
- Interfaz Gráfica de Usuario (aplicación de software privativa)
- Interfaz de Línea de Comandos (telnet, ssh)
- Interfaz de software integrada en el sistema (cuando el AP/cliente es un computador o un teléfono inteligente con una pantalla y su propio sistema operativo).

Interfaces de Usuario: GUI (página web)

Este sistema se usa en Linksys, Ubiquiti y la mayoría de los AP más modernos. Una vez que usted se conecta con el AP, interactúa con el dispositivo usando un navegador normal.

Ventajas: trabaja con la mayoría de los navegadores y sistemas operativos.
Desventajas: la interfaz estática no refleja los cambios inmediatamente; hay una retroalimentación deficiente; puede ser incompatible con algunos navegadores; necesita una configuración TCP/IP funcionando.

Algunas implementaciones recientes (ver Ubiquiti en la figura siguiente) son muy buenas y usan características de red dinámicas y modernas para ofrecer retroalimentación y herramientas avanzadas.



Figura SCH 6: Interfaz de usuario Ubiquiti

Interfaces Gráfica de Usuario: GUI (aplicación de software)

En este caso, se va a necesitar un software para interactuar con el dispositivo. Este sistema se usa en Mikrotik (se llama Winbox), Apple (llamado Airport Utility), Motorola (Canopy) y muchos AP viejos.
Ventajas: interfaces a menudo atractivas y poderosas; permite configuración en grupo de múltiples dispositivos.

Desventajas: soluciones privativas; normalmente para un solo sistema operativo; el software debe instalarse antes de empezar la configuración.
A continuación se muestra Mikrotik Winbox, una solución muy poderosa que puede manejar redes grandes.

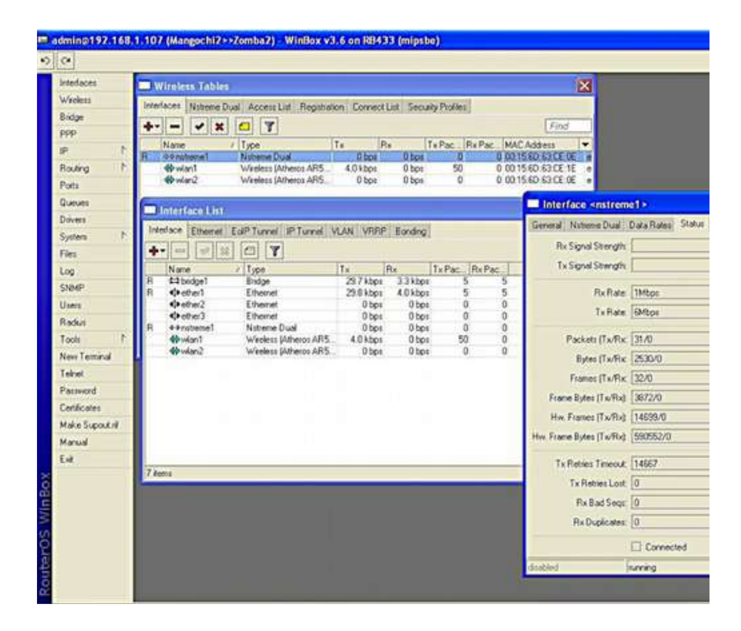


Figura SCH 7: Win Box de Mikrotik

Interfaces de usuario: Interfaz de Línea de Comando (a veces llamada text shell)

En este caso usted se conecta con el dispositivo usando una conexión serial o conexión Ethernet, por medio de telnet o ssh. Ssh es mucho más conveniente que telnet desde el punto de vista de la seguridad (este último debe evitarse en la medida de lo posible).
La configuración se efectúa con órdenes ejecutadas en el sistema operativo del anfitrión, normalmente una variación de Linux o un sistema operativo propietario como se muestra más adelante.

Este sistema lo usa Mikrotik (se llama RouterOS), Ubiquiti (AirOS), AP de gama alta (high-end) (Cisco), y AP incrustados con basados en PC.

Ventajas: muy poderoso ya que puede utilizar guiones (scripts).

Desventajas: difícil de aprender.

```
root@wildnet-1: ~ — ssh — 80×24
root@wildnet-1:~# ssh ubnt@192.168.254.32
ubnt@192.168.254.32's password:


BusyBox v1.11.2 (2009-10-23 17:52:21 EEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

XM.v5.0.2# help

Built-in commands:
-------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help jobs kill let local printf
        pwd read readonly return set shift source test times trap true
        type ulimit umask unalias unset wait

XM.v5.0.2#
```

Figura SCH 8: Interfaz de Línea de Comandos (CLI)

Configuración del Punto de Acceso (AP)

Antes de configurarlo, recuerde:

- Comience desde un estado conocido, o reinicie el dispositivo a la configuración de fábrica (siempre una buena idea).
- Conectarse al dispositivo mediante Ethernet es generalmente más fácil que por vía inalámbrica. La mayor parte de los dispositivos con una GUI (Interfaz Gráfica de Usuario) de red tienen una configuración IP por defecto en la red 192.168.0.0, pero esto no es una regla. !Lea el manual!
- Si conviene, actualice el firmware hasta la última versión estable, (pero con cuidado).
- Cambie en primer lugar el nombre de usuario del/la administrador/a y la contraseña.
- Cambie el nombre del dispositivo y déle un nombre que lo identifique claramente (por ejemplo "AP_salón_conferencia_3", o "hotspot_área_pública". Esto le ayudará a reconocer el AP en el futuro cuando vaya a conectarse con él en la red.

- La actualización del firmware es a menudo una operación de riesgo; asegúrese de tomar todas las precauciones antes de intentarlo, como conectar el dispositivo y el computador a un UPS, y luego no realizar la actualización mientras ejecuta otras tareas en el computador; y controle que tenga una imagen binaria válida del firmware. LEA LAS INSTRUCCIONES CON CUIDADO. Si el procedimiento falla, usted puede quedarse con un dispositivo inutilizado irrecuperable (llamado “ladrillo”).
- Recuerde anotar por escrito (y guardar en sitio seguro) todas las configuraciones, especialmente el nombre de usuario y contraseña del(la administrador/a.

Configuración de la capa AP - IP

Si tiene confianza en lo que está haciendo, puede hacer la configuración IP después de la inalámbrica para evitar la reconfiguración y reconexión de su PC o portátil. Pero de esta manera, si usted comete cualquier error bien sea en la configuración cableada o inalámbrica, puede terminar con un AP sin acceso. Nuestra recomendación es que la configuración más delicada se haga paso a paso controlando el estatus del dispositivo en cada paso. Y recuerde escribir y guardar en un sitio seguro todas las configuraciones IP.
Configure la interfaz Ethernet del AP de acuerdo con las características de la red cableada:

- Dirección/máscara de red/ pasarela o DHCP de la IP.
- Dirección(es) DNS
- Chequee doblemente las nuevas configuraciones y aplíquelas (algunas veces hay que reinicializar el AP).
- Ahora usted podría necesitar reconfigurar su PC/portátil para coordinarlo con las nuevas configuraciones de Ethernet, y reconectarlo al AP.
-

Configuración del AP —capa física

- Configure el modo: máster (o punto de acceso o estación base). El modo del dispositivo puede ser configurado normalmente como “master” (también llamado “punto de acceso” o “estación base” o “BS”); modo “cliente” (también llamado “administrado”, o “estación”, o “estación cliente” o “CPE”), “monitor”, “WDS” (por Wireless Distribution System), y pocas variantes más.

- Configure el SSID (Service Set Identifier, es el nombre de hasta 32 caracteres de la red inalámbrica creada por el AP). Aquí es mejor utilizar un nombre que tenga significado. Recuerde que la seguridad por medio del ocultamiento no es seguridad real; por eso, un SSID oculto, falso o aleatorio no añaden seguridad a su red.
- Configure el canal inalámbrico de acuerdo con las regulaciones locales y el resultado de la prospección del sitio (site survey).
- No use un canal que esté ya ocupado por otro AP u otras fuentes de radio frecuencia. Usted debería haber planificado el canal previamente en la fase de diseño de la red. La escogencia del mejor canal es a veces difícil y a lo mejor hay que hacer una inspección de sitio con software especializado (rastreadores inalámbricos) o hardware, como los analizadores de espectro (por ej. WiSpy de Metageek y AirView de Ubiquiti).
- Configure la potencia de transmisión y la velocidad de la red (estos valores pueden fijarse en "automático" en algunos dispositivos. El valor para la potencia de transmisión está sujeto a regulaciones locales. Controle previamente el valor máximo que permite la ley y trate siempre de usar el valor mínimo que satisfaga sus necesidades para evitar la interferencia con otras redes (incluida la suya).

La elección de la velocidad de la red esta limitada por los valores de los estándares 802.11a/b/g/n (hasta 54 Mbps), pero algunos vendedores han creado extensiones de estos estándares (llamados modos "turbo") de 100Mbps o más. Estas extensiones no son estándar y podrían no funcionar con equipos provenientes de otros vendedores.

Si escogemos el modo "backwards compatibility" (lo que implica compatibilidad con las redes 802.11b y 802.11g) se va a reducir el caudal neto global disponible para los clientes más veloces. El AP debe enviar el preámbulo a una tasa más baja para los clientes 802.11b y la comunicación real entre el cliente y el AP ocurrirá a velocidades de 802.11b.
Esto toma más tiempo y retrasa a los clientes 802.11g que podrían ser más rápidos.

Configuración del AP —seguridad

Las escogencias de seguridad suelen ser complicadas y puede ser difícil establecer un balance entre una buena protección contra usuarios no intencionales y un acceso fácil para los usuarios autorizados.

Las medidas de seguridad más complejas necesitan una configuración también más compleja y software adicional.
Configure las características de seguridad de la red:

- Sin encriptación (todo el tráfico va sin cifrar)
- WEP (*Wired Equivalent Privacy*): tanto la clave de 40 como la de 104 bits son vulnerables y por lo tanto WEP no debería emplearse.
- WPA / WPA2 (*WiFi Protected Access*): PSK, TKIP y EAP
- Activar o desactivar (ocultar) la emisión SSID (baliza). SSID ocultos o el filtrado de MAC no añaden mucha seguridad, son difíciles de mantener y son una fuente de problemas para usuarios inexpertos de la red.
- Active o desactive una Lista de Control de Acceso (basada en las direcciones MAC de los clientes). EL filtrado de MAC es una medida de seguridad débil. Un cliente malicioso puede captar paquetes de datos y averiguar cuáles son las direcciones MAC que tienen derecho a asociarse a ellos. Luego, puede cambiar su propia dirección MAC por una de las aceptadas y "engañar" al punto de acceso.

Para más información sobre el diseño de la seguridad de su red inalámbrica , vaya al capítulo **Seguridad para Redes Inalámbricas**.

Configuración del AP —enrutamiento/NAT

Las configuraciones avanzadas de la capa IP y de enrutamiento suelen incluirse en los AP modernos. Estas pueden comprender funcionalidad para el enrutamiento y Traducción de las Direcciones de Red (NAT en inglés), además de "puenteo" (*bridging*) básico.

La configuración avanzada para IP incluye:

- Enrutamiento estático
- Enrutamiento dinámico
- NAT (enmascaramiento y redireccionamiento de puertos)
- Cortafuegos
- Algunos AP pueden funcionar de servidores de archivos o de impresión (HD externos e impresoras pueden conectarse por USB)

Configuración del AP —avanzada

Hay algunas configuraciones avanzadas para su AP dependiendo del modelo, vendedor, *firmware,* etc.

- Intervalo de baliza (beacon interval)
- El mecanismo RTS/CTS. RTS/CTS (ready to send, clear to send) puede ayudar con los problemas de nodos escondidos (clientes que pueden "oír" el AP pero no a otros clientes, lo que va a crear interferencias).
- Fragmentación. Configurar la fragmentación puede ser útil para aumentar el rendimiento en el caso de zonas de señal baja, con cobertura marginal o en enlaces largos.
- Solidez ante interferencias
- Extensiones a los estándares WiFi proporcionadas por el vendedor
- Otras configuraciones para enlaces de larga distancia (10 a 100 kilómetros) y mejor seguridad.

Configuración del cliente

La configuración del lado del cliente es más sencilla:

- Configure el modo: **client** (o **administrado, estación, estación cliente, CPE**)
- Configure el SSID de la red a la que se va a unir
- El canal, la velocidad y otros parámetros serán fijados automáticamente para coordinarlos con el AP
- Si WEP o WPA se activa en el AP, tendrá que ingresar la contraseña (clave) correspondiente
- Los clientes pueden tener especificaciones adicionales (a menudo fijadas por el vendedor). *Por ejemplo, algunos clientes pueden configurarse para asociarse solamente con un AP que tenga una dirección MAC determinada.*

Sugerencias – trabajo en exteriores

- Trate de configurar los dispositivos (tanto AP como clientes) con bastante antelación en un sitio cómodo, como un laboratorio. El trabajo en exteriores es más difícil y conduce a errores (**configuración in situ** = problemas)

- Si **debe** configurar en exteriores, asegúrese de tener suficiente carga de batería para su portátil, de llevar toda la información necesaria (**en papel** además de formato electrónico) y de llevar un cuaderno para anotar. La buena documentación es imprescindible para el mantenimiento futuro en el campo.

Solución de Problemas

- Organice su trabajo en pasos lógicos y sígalos.
- Lea el manual, estudie el significado de los parámetros, haga tests y experimentos (!sin miedo!).
- En caso de problemas, haga un reset total (condiciones de fábrica) y pruebe de nuevo.
- Si el problema persiste, pruebe de nuevo **cambiando un parámetro o variable a la vez.**
- ¿Todavía no funciona? Pruebe a buscar en la web con palabras clave importantes (nombre del dispositivo, etc.); busque en los foros o en los sitios web del vendedor/fabricante.
- Actualice el *firmware* a su última versión.
- Si todavía tiene problemas pruebe con un cliente o un AP diferentes para descartar un problema de hardware con el original.

12. INSTALACIÓN EN INTERIORES

Introducción

Las ediciones anteriores de este libro se han enfocado en instalaciones inalámbricas para áreas extensas en exteriores como medio de conectar comunidades a Internet. Sin embargo, con la disponibilidad de puntos de acceso WiFi a bajo precio y la proliferación de dispositivos portátiles que usan conexión inalámbrica, Wifi se ha convertido en el estándar de facto para redes de interiores en empresas y escuelas. Este capítulo presenta los principales puntos de enfoque cuando tenga que escoger o instalar redes WiFi para interiores.

Preparación

Antes de instalar una LAN inalámbrica es una buena idea pensar con detenimiento sobre algunos detalles:

- ¿Qué planea usted hacer con la red inalámbrica? ¿Es un complemento para una red cableada o es un reemplazo de esta? Va a ejecutar aplicaciones en esta red que no toleran retardo o que son sensitivas a las variaciones de ancho de banda (como voz, o videoconferencias)?
- La diferencia principal entre redes inalámbricas de interiores y exteriores es la absorción y reflexión de las ondas de radio que va a ocasionar el edificio mismo. ¿Cuáles características del edificio tienen que tomarse en cuenta? ¿Las paredes contienen metal, agua o concreto pesado? ¿Las ventanas tienen metal (por ej. capas de metal o rejillas)? ¿El edificio es largo y estrecho, o es compacto?
- ¿Se espera que los usuarios permanezcan casi siempre en sus sitios, o van a estar en movimiento frecuente? Cuando se mueven es importante tener un traspaso (*handover)* ininterrumpido, (es decir, un *handover* tan rápido que no se note la interrupción en una llamada de voz).
- ¿Hay buenos sitios para colocar los Puntos de Acceso? ¿Hay enchufes cableados y electricidad de disponibilidad inmediata para los puntos de acceso? ¿Es estable la electricidad? Si no lo es, podría necesitar fuentes de energía estable solar/batería y/o UPS incluso en interiores.

- ¿Hay fuentes de interferencia como puntos de acceso ad hoc traídos por los usuarios, dispositivos bluetooth o microondas?

Requisitos de ancho de banda

El primer paso en el diseño inalámbrico de interiores es determinar las necesidades en términos del número de usuarios que hay que atender simultáneamente, el número de dispositivos y el tipo de aplicaciones que estos ejecutan.
También es importante entender la distribución de los usuarios. Los salones de conferencias o de reuniones tienen diferentes patrones de uso que los corredores.
Una red inalámbrica que se usa con poca frecuencia y que sirve a pocos usuarios es fácil de implementar y no dará muchos problemas.
El problema empieza cuando aumenta el número de los usuarios y la frecuencia de uso. Por lo tanto, nos concentraremos en redes inalámbricas de alta densidad.
A continuación les damos una idea de los requisitos de ancho de banda para algunas aplicaciones comunes:

navegar en la red:	500 - 1000 kb/s
Audio:	100 - 1000 kb/s
video en tiempo real:	1 - 4 Mb/s
compartir archivos :	1 - 8 Mb/s
respaldo del dispositivo:	10 - 50 Mb/s

Las instalaciones típicas de una oficina se diseñan para servir 20-30 usuarios por celda y tienen 1 punto de acceso por 250-500 metros cuadrados; pero, como mencionamos antes, esto puede no ser suficiente dependiendo de las características del medio.

En un ambiente denso puede haber hasta un dispositivo por 20 m2.
En pocas palabras, se necesita calcular el caudal (throughput) necesario por área de cobertura. Así que si se tienen 10 usuarios en un área de 20 m2, de los cuales 8 están navegando en Internet y 2 están viendo videos online, usted va a necesitar 8 * 1000 kb/s + 2 * 4000 kb/s = 16000 kb/s para el área de 100 m2, o 160 kb/s por m2.

Frecuencias y tasas de datos

Las soluciones de 2.4 GHz y 5 GHz difieren en aspectos claves. La banda de 2.4 GHz tiene un mayor alcance y una menor atenuación y se usa en la mayoría de los dispositivos.
El mayor defecto de la banda de 2.4 GHz es que hay sólo 3 canales que no se solapan, lo que limita mucho el número de puntos de acceso que pueden colocarse en un área determinada.

Esto es lamentable ya que hacer celdas más pequeñas (lo que se logra haciendo que los AP transmitan con menos potencia) es la manera más sencilla de lograr más caudal (throughput) por superficie.

Nota: algunas veces se aconseja tener 4 canales ligeramente solapados, pero la investigación demuestra que esto va a disminuir el rendimiento. En líneas generales, el rendimiento se deteriora rápido cuando hay solapamiento de canales (interferencia co-canal).
Por otra parte, la banda de 5 GHz, tiene el peor alcance, pero en la mayor parte del mundo tiene 20 canales, lo que hace más fácil las instalaciones sin la interferencia desde los canales adyacentes.
Otro elemento importante es la elección del estándar WiFi considerando que el caudal promedio en Mb/s para las tecnologías más comunes es:

11b:	7.2 Mb/s
11g:	25 Mb/s
11a:	25 Mb/s
11n:	25 - 160 Mb/s

Debe notarse que el rendimiento cae cuando por ejemplo los dispositivos 802.11b y 11g están servidos por el mismo AP. En una red donde los dispositivos cliente usan una mezcla de 802.11g y 11b, el AP reducirá su operación a las velocidades más bajas.
La elección de 5 GHz es mejor para redes de alta densidad y alto rendimiento. Como de todas maneras se quiere limitar la cobertura de cada AP a un área pequeña y bien definida, la atenuación de la señal causada por paredes, etc. es más bien una ventaja que un problema. También vale la pena considerar la utilización de 2.4 GHz para la mayoría de los dispositivos en combinación con 5 GHz par los “dispositivos importantes”.

Puntos de Acceso, elección y ubicación

Cuando se trata de elegir Puntos de Acceso (AP) para redes inalámbricas interiores hay básicamente dos elecciones de arquitectura: "basada en controlador" y "clientes pesados". Los "clientes pesados" son AP autónomos que incorporan toda la inteligencia para manejar una red WiFi (para escoger las SSID, métodos de cifrado, enrutar/conmutar, etc.).
La solución basada en controlador, en cambio, tiene puntos de acceso con una funcionalidad mínima para el servicio inalámbrico junto con un controlador central común para los AP del área. El controlador central tiene también toda la inteligencia y todo el tráfico que le dirige el AP.
La elección entre estas dos arquitecturas es un compromiso entre costo, facilidad de manejo y escalabilidad. Se puede decir en general que a mayor complejidad del ambiente y a mayor tamaño de la red, más atractiva se hace la solución basada en controlador.

Los Puntos de Acceso deben en general colocarse en las áreas con una alta densidad de usuarios; la señal va a "regarse" lo suficiente como para servir las áreas menos densas. Sin embargo, el rendimiento general del sistema va a estar determinado más que todo por los clientes, no por la ubicación del AP. A pesar de que es importante, la colocación del AP no puede añadir mucho al rendimiento global del sistema. Otras fuentes de radio en las bandas WiFi tienen gran influencia en el rendimiento de la red WiFi, así que, en la medida de lo posible, aísle el AP de otras fuentes de radio por medio de paredes, techos y la propia gente, usada como "escudos".

También es posible usar antenas externas para mejorar el rendimiento. Las antenas omnidireccionales son las más comunes en este caso; ellas dan un área de cobertura casi circular alrededor del AP. Sin embargo, para la mayoría de los casos en interiores, los AP se instalan en las paredes, techos o columnas por lo que las antenas omnidireccionales no son una buena opción teniendo en cuenta hacia donde van las ondas de radio y dónde están los usuarios.

Para los casos en los que el AP no está en el centro del área que se debe cubrir, la alternativa son las antenas direccionales. Por ejemplo, algunos hoteles o centros de conferencias colocan antenas direccionales pequeñas en las esquinas de áreas grandes y abiertas para proporcionar una cobertura en "paraguas" de grandes espacios.

Tenga en cuenta que la cantidad de reflexión que normalmente se encuentra en ambientes internos hace difícil el control completo de una cobertura específica.

Los Puntos de Acceso pueden montarse en el techo, en las paredes o en muebles y cada elección va a tener diferentes características. La posición en el techo va a ofrecer una buena cobertura tipo manta; en las paredes vamos a tener el AP más cerca de los usuarios, y bajo las mesas, sillas o dentro de los muebles se puede aprovechar el aislamiento natural para crear pequeñas celdas con poca interferencia desde los AP vecinos; sin embargo, en este caso puede haber preocupación sobre los posibles efectos nocivos de la radiación emitida.
Por último, para redes que exigen alto rendimiento, los AP con tecnología de antenas inteligentes adaptables puede ser una opción. Son costosas, pero ofrecen la ventaja de adaptar de manera dinámica la señal de radio a la ubicación de los usuarios: van a dirigir las ondas de radio hacia donde se necesitan en cada momento.

SSID y Arquitectura de Red

Las redes de interiores suelen servir a usuarios simultáneos. Los complejos grandes como un campus universitario constan normalmente de varios edificios, cada uno con su red interna, y redes externas entre ellos. Por lo tanto, hay que hacer una buena planificación de sus SSID. Recuerde que la SSID define el dominio de transmisión en Capa 2 de la red. La planificación de su SSID implica jugar con la arquitectura de Capa 3 de su red. Si usted quiere que los usuarios circulen sin interrupción por toda el área de su red, entonces todos los AP deberían tener la misma SSID, por ejemplo “UniversidadInalámbrica”, o “eduroam” en el caso de que la universidad quiera participar de los servicios globales de *roaming* que ofrece eduroam.
Sin embargo, los usuarios que permanecen dentro de una SSID no van a necesitar o a solicitar nuevo contrato DHCP, así que tendrá que acomodar todos los usuarios dentro de UNA SOLA subred Capa 3.
Para un campus grande, esto puede precisar una subred plana y grande para todos los usuarios inalámbricos. Esta es una situación de compromiso: se puede tener subredes enormes con roaming ininterrumpido, o tener una subred de arquitectura más manejable con SSID separadas, como “Biblioteca”, “Sala de Conferencias”, “Cafetería”, etc.

Post Instalación

Ahora que tiene la infraestructura en su lugar hay que asegurarse de que todo funcione como previsto y de que se mantenga así. Esto puede lograrse haciendo como una prospección de sitio: con mediciones de intensidad de las señales y de los caudales. Pero en resumidas cuentas la razón principal para instalar una red inalámbrica es servir a los/las usuarios/as de la misma, de tal manera que escuchar las quejas o problemas que tengan es igual de importante. La demanda cambia en continuación así como las actualizaciones. Es importante mantenerse al día con las necesidades de los usuarios y acoplar estas con actualizaciones programadas de la tecnología que se está utilizando.

13. INSTALACIÓN EN EXTERIORES

A pesar de que la tecnología WiFi se diseñó para redes de área local, su impacto en los países en desarrollo es más importante en aplicaciones de larga distancia.

Sin embargo, la penetración de la fibra óptica en los países en desarrollo no es lo suficientemente amplia ni está cerca de cubrir las necesidades de la mayoría de las ciudades. Y los costos de su expansión no cumplen a menudo, en un período razonable de tiempo, con los objetivos de Retorno de Inversión a que aspiran las empresas de telecomunicaciones. A pesar de esto último, las tecnologías inalámbricas han tenido más éxito en los países en desarrollo y el potencial para aumentar su expansión es enorme.
Telcos ha instalado enlaces tradicionales de radio por microondas en la mayoría de los países. Esta es una tecnología madura que ofrece una disponibilidad y confiabilidad que alcanzan el 99.999%. Sin embargo, estos sistemas cuestan miles de dólares y necesitan personas especialmente entrenadas para su instalación.

Los sistemas satelitales han demostrado ser eficientes en tráfico de radiodifusión la TV y algunas otras aplicaciones. No obstante, estas soluciones son todavía muy caras para tráfico bidireccional, mientras que WiFi es una opción muy rentable para redes exteriores punto a punto, así como en redes de acceso típicas con una Estación Base (BS) que sirve a muchos Clientes/CPE (punto a multipunto). En este capítulos nos enfocaremos en los enlaces de exteriores de larga distancia punto a punto.
Hay dos obstáculos grandes que hay que salvar antes de utilizar WiFi como solución para largas distancias: limitaciones de presupuesto de potencia y de temporización. Las limitaciones restantes para su uso en largas distancias se refieren a la existencia de línea visual de radio entre los dos extremos del enlace y la vulnerabilidad a la interferencia en la banda sin licencia.
La primera puede solventarse a menudo aprovechando las elevaciones del terreno o usando torres para sortear obstáculos como la curvatura terrestre o para dejar libre la zona de Fresnel.
Para aplicaciones en interiores la línea visual no hace falta puesto que las estaciones están muy cerca unas de otras y casi todos los obstáculos pueden sortearse por medio de reflexiones en las paredes, el techo, etc.

Pero para largas distancias, la línea visual es completamente imprescindible. La limitación de interferencia es menos importante en áreas rurales y se puede aliviar migrando a la banda de 5 GHz, menos congestionada. El problema del presupuesto de potencia puede manejarse utilizando antenas de ganancia alta y radios sensibles y potentes conectados directamente a la antena para evitar pérdidas en los cables de RF. Los problemas de sincronía tienen que ver con las técnicas de acceso a los medios. WiFi emplea una técnica aleatoria de acceso para compartir el medio de comunicación. Esto lo vuelve susceptible a colisiones que no pueden detectarse por el aire, y por lo tanto, el transmisor depende de recibir una confirmación de cada trama recibida con éxito. Si después de un tiempo específico que se llama "*ACKtimeout*" (tiempo de confirmación vencido) no se recibe confirmación, el transmisor vuelve a mandar la trama. Y como el transmisor no va a mandar una nueva trama hasta que no se haya recibido el ACK de la precedente, el "*ACKtimeout*" debe mantenerse corto. Esto funciona bien en el caso original de uso de WiFi (redes interiores) en el cual el tiempo de propagación de 33.3 microsegundos es insignificante, pero no sirve cuando se trata de enlaces de algunos kilómetros. A pesar de que muchos dispositivos WiFi no prevén la modificación del *ACKtimeout,* los equipos nuevos para uso en exteriores (o algunos *firmware* producidos por otras personas como Open WRT) si lo permiten, a menudo a través de un campo llamado *distancia* que se encuentra en la Interfaz Gráfica de Usuario o GUI (*Graphical User Interface*).
Cuando se cambia este parámetro se obtiene un caudal (*throughput*) razonable que de todas maneras va a disminuir con la distancia. La duración de la ranura de tiempo de la ventana de contención también debe adaptarse a las distancias más grandes. Otros fabricantes han escogido migrar de acceso aleatorio a Acceso Múltiple por División de Tiempo, o TDMA (***Time Division Multiple Access*****).** TDMA divide el acceso asignado a un determinado canal en múltiples franjas de tiempo y asigna estas franjas a cada nodo de la red. Cada nodo transmite solamente en su franja asignada evitando de esta manera las colisiones. Esto ofrece grandes ventajas en un enlace punto a punto que así no necesita las confirmaciones (ACK) puesto que las estaciones se turnan para transmitir y recibir. A pesar de que este método es eficiente, no cumple con los estándares WiFi. Por eso algunos fabricantes lo ofrecen como un protocolo patentado opcional junto con los estándares WiFi. Por ejemplo WiMAX y algunos protocolos patentados (como Nstreme de Mikrotik, o AirMAX de Ubiquiti Networks) usan TDMA para evitar los problemas de temporización ACK.

El estándar 802.11 define la sensibilidad del receptor como el nivel de recepción de la señal requerido para garantizar una Tasa de Error de Bits o BER (*Bit Error Rate*) por debajo de 10^{-5}. Esto determina la cantidad de potencia por bit necesaria para contrarrestar el ruido ambiente sumado al ruido generado por el mismo receptor. A medida que la cantidad de bits/segundo transmitidos aumenta, se necesitará más potencia de recepción para proporcionar la misma potencia por bit. Por lo tanto, la sensibilidad del transmisor disminuye a medida que la tasa del transmisor aumenta. Y así, para mantener la misma relación señal/ruido al aumentar la distancia, el caudal disminuye. Para largas distancias se debería escoger tasas bajas de transmisión de datos para compensar la reducción de la potencia de la señal ocasionada por la distancia.

¿Qué se necesita para un enlace de larga distancia?

Hay cuatro aspectos que deben considerarse para adaptar dispositivos WiFi a largas distancias: incremento del alcance dinámico del radio; aumento de la ganancia de la antena; disminución de la pérdida del cable de la antena; y las previsiones para el tiempo de propagación de la señal.

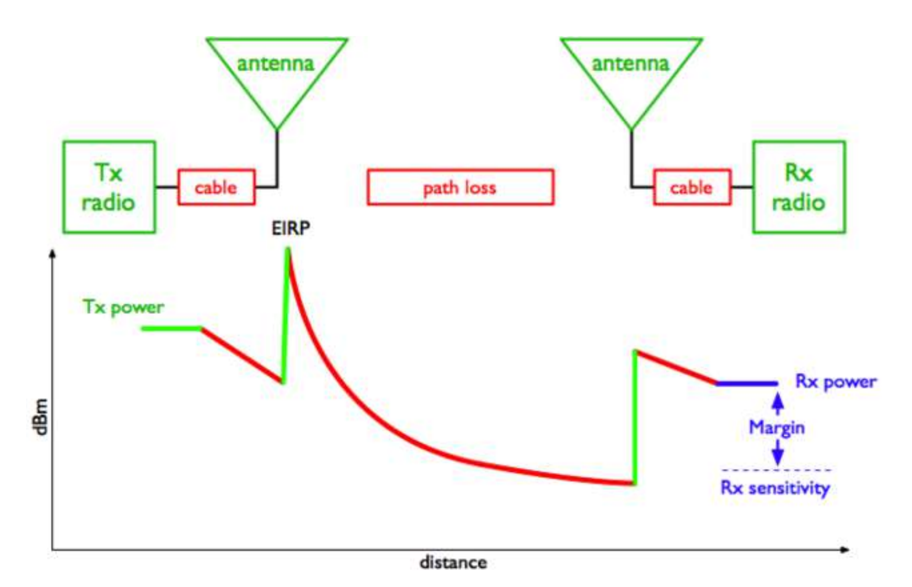


Figura IE 1: Potencia en dBm vs. distancia en un enlace de radio (Presupuesto de Potencia)

El gráfico anterior muestra el nivel de potencia en cada punto de un enlace inalámbrico. El transmisor proporciona cierta cantidad de potencia. Una pequeña cantidad de esta se pierde en atenuación entre el transmisor y la antena, en el cable RF o guía de onda. La antena, entonces, enfoca la potencia y proporciona una ganancia. En este punto, la potencia tiene el valor máximo posible para el enlace. Este valor se denomina Potencia Irradiada Isotrópica Equivalente, EIRP (*Equivalent Isotropic Radiated Power*) puesto que corresponde a la potencia que un transmisor tendría que emitir si la antena no tuviera ninguna ganancia.
Entre las antenas transmisora y receptora hay un espacio libre y pérdidas ambientales que aumentan con la distancia entre los extremos del enlace. La antena receptora da alguna ganancia adicional. Y hay una pequeña pérdida entre la antena receptora y el radio receptor.

Si la potencia recibida en el extremo lejano es mayor que la sensibilidad de recepción del radio, el enlace es posible. Si se aumenta la potencia de transmisión se puede incurrir en violaciones de las regulaciones específicas del país.

Aumentar la ganancia de la antena es el método más efectivo para mejorar el alcance. Asegúrese de que el radio que va a usar tenga conectores para la antena externa (algunos dispositivos tienen una antena incorporada, o no removible).
Disminuir la pérdida en los cables de la antena es todavía algo que se debe hacer, y la forma más drástica de hacerlo es colocando el radio afuera, directamente conectado a la antena, usando una caja impermeable. A menudo esto lleva a alimentar el radio usando PoE (*Power over Ethernet*).
Mejorar la sensibilidad del receptor implica escoger un modelo con mejor rendimiento, o transarse por velocidades de transmisión bajas con sensibilidad más alta.
A pesar de que las antenas de alta ganancia son caras, en muchos países se puede encontrar todavía antenas parabólicas que ya no se usan y que pueden modificarse para las bandas WiFi.
En un mundo perfecto usaríamos las antenas de mayor ganancia con los radios más potentes y sensibles que exista. Sin embargo, esto no es posible debido a consideraciones prácticas. Los amplificadores introducen más puntos de fallas y además podrían violar las regulaciones de máxima potencia permitida en le país, y añadir ruido a la recepción; en consecuencia deberían evitarse.

Hay fabricantes que ofrecen transmisores de alta potencia de hasta 1 W de potencia de salida que podrían usarse en lugar de amplificadores en países donde sea legal. En general, es mejor usar antenas de alta ganancia que transmisores de gran potencia. Una ganancia de antena más grande va a ayudar tanto en la transmisión como en la recepción con un doble impacto positivo para le presupuesto del enlace. También va a ocasionarle menos interferencia a otros usuarios, a recibir menos interferencia de otros usuarios y a limitar los efectos multi-trayectoria. Sin embargo, una ganancia alta también implica un ancho de haz muy estrecho que va a exigir la aplicación de técnicas de alineamiento.

Alineamiento de Antenas

Para distancias cortas, cuando la antena correspondiente es visible, el procedimiento de alineación se reduce a orientar la antena hacia la dirección de la correspondiente en el plano horizontal (azimut) y en el vertical (elevación). Esto debería bastar para establecer la conexión. Una vez establecida esta, se pueden hacer ajustes finos leyendo el RSSL (*Receiver Signal Strength Level*), o Nivel de Potencia de la Señal del Receptor en el radio local. Este valor lo proporciona la interfaz del usuario y se puede obtener también en programas como *netstumbler.* El procedimiento consiste en mover la antena en pequeños pasos mientras se lee el RSSL. No toque la antena cuando haga la lectura porque su cuerpo va a afectar la medición. Una vez satisfechos con la obtención del máximo nivel, se repite la operación en el plano vertical moviendo la antena primero hacia arriba y luego hacia abajo hasta obtener un valor máximo de potencia recibida. En este punto, apretamos los tornillos que fijan la antena. Esto es todo lo que se necesita para orientar un dispositivo cliente hacia un Punto de Acceso o Estación Base. Si usted tiene un enlace punto a punto, debe repetir el mismo procedimiento en el otro extremo del enlace.

Para distancias largas y cuando el otro extremo del enlace no es visible necesitamos pasos adicionales. En primer lugar, a partir de las coordenadas de ambos extremos debemos obtener la dirección horizontal o rumbo (*bearing*) para apuntar la antena. Luego usamos una brújula para determinar la dirección hacia la cual se va a orientar la antena. Recuerde que, en general, hay una diferencia entre el rumbo magnético medido por la brújula, y el rumbo geográfico obtenido a través de las coordenadas de los extremos del enlace o en un mapa.

La diferencia entre ambos se llama declinación magnética, y puede ser importante en algunos lugares por lo que debe tomarse en cuenta para orientar la antena con precisión. La Figura IE 2 muestra la diferencia de 10° entre el norte magnético de la brújula y el norte geográfico o verdadero norte indicado en la placa de bronce.



Figura IE 2: Diferencia entre el Norte Magnético y el Geográfico en El Baúl, Venezuela, 2006

Recuerde que el hierro y otros metales magnéticos afectarán la lectura de la brújula así que manténgase alejado de ellos cuando tome las medidas.
Si la antena se debe montar en una torre de acero puede ser imposible lograr una lectura precisa cerca de la misma. En este caso, aléjese a una cierta distancia, use la brújula para determinar la dirección a la que se debe orientar la antena y luego trate de localizar un objeto fácilmente reconocible que se pueda usar como referencia para orientar la antena hacia él más tarde. Puesto que el ancho del haz de una antena muy directiva podría ser de pocos grados, después de apuntar con la brújula tenemos que hacer ajustes finos para lograr la orientación adecuada, por medio de la medición de la potencia de la señal recibida.
Lamentablemente, el Indicador del Nivel de Señal Recibida, RSSL, indicado por el software del radio sólo trabajará después de que un paquete apropiado haya sido recibido satisfactoriamente y descodificado, y esto sólo ocurrirá cuando la antena esté bien orientada.

Entonces, necesitamos un instrumento que nos dé la potencia de la señal recibida independientemente de la modulación que pueda tener. Este instrumento es el Analizador de Espectro.
Hay una gran variedad de ellos en el mercado algunos de los cuales cuestan miles de dólares, per si sólo nos interesan las bandas WiFi, podemos adoptar soluciones económicas como las siguientes:
"RF Explorer" ofrece dispositivos económicos para varias bandas de frecuencia. El "RF Explorer modelo 2.4G" cuesta 120$ en:
http://www.seeedstudio.com/depot/-p-924.html?cPath=174
y es un sistema autónomo que puede medir señales desde 2.4 a 2.485 GHz, con una sensibilidad de -105 dBm. Tiene un conector SMA para la antena, por lo tanto es adecuado para alineación de antenas.
"WiSpy" es un analizador de espectro en una llave USB que se conecta a una portátil. Usted va a necesitar los modelos con conectores SMA RP. En el mercado hay uno para 2.4 GHz de precio moderado, y otro que cubre ambas bandas, la de 2.4 y 5 MHz por 600$ en www.metageek.net.

"Ubiquiti Networks", en www.ubnt.com, solía vender analizadores de espectro de llave USB para 2.4 GHz en 70$. Desafortunadamente parece que ellos descontinuaron este producto después de incorporar la capacidad de analizador de espectro a sus radios de la serie M. Así que cuando use estos radios, se puede aprovechar su herramienta de alineación “airView”. En principio, uno de estos radios económicos como el “Bullet M” que viene con un conector macho N puede usarse para alinear antenas para otros radios en las bandas de 2.4 y 5 GHz. Sin embargo, la señal modulada digitalmente que transmiten los radios WiFi no es adecuada para alineación de antenas porque su potencia se dispersa en la banda de 20MHz. Para alineación de antenas, se necesita una frecuencia única con una potencia de salida estable. Este tipo de señal es producida por un generador de señal de microondas, pero estos son muy caros.
El "RF Explorer modelo 2.4G" incorpora un generador de señal 2.4 GHz, pero la potencia máxima de salida de 1 dBm no es adecuada para alineación de antenas para distancias largas. En su lugar, hemos replanteado los dispositivos llamados “video senders”, diseñados para transmitir señales de video, y que actúan como fuentes poderosas de señales de microondas de frecuencia única, cuando so se aplica modulación.
Estos dispositivos están disponibles para las bandas de 2.4 y 5 GHz con potencia de salida de hasta 33 33 dBm.

Para nuestros propósitos hay que comprar un modelo con un conector de antena para pegarle nuestra propia antenas.

Hay muchos vendedores para escoger, por ejemplo:
http://www.lightinthebox.com/Popular/Wifi_Video_Transmitter.html

Como ejemplo de enlace de larga distancia que usa dispositivos WiFi modificados podemos mencionar un experimento hecho en Venezuela en abril del 2005 entre Pico del Águila (8.83274638° N, 70.83074570°W,4100 m de elevación) y El Baúl (8.957667° N, 68.297528° W, 155 m de elevación).
Usando el software de Radio Mobile, encontramos que la distancia a El Baúl es de 280 km, el azimut de 97º, el ángulo de elevación de la antena de -2,0º y el lugar en el cual el haz está más cerca del suelo está a 246 km, donde despeja 1.7 veces la primera zona de Fresnel a la frecuencia de 2.412 GHz.

La Fig. IE 3 muestra la salida del programa:

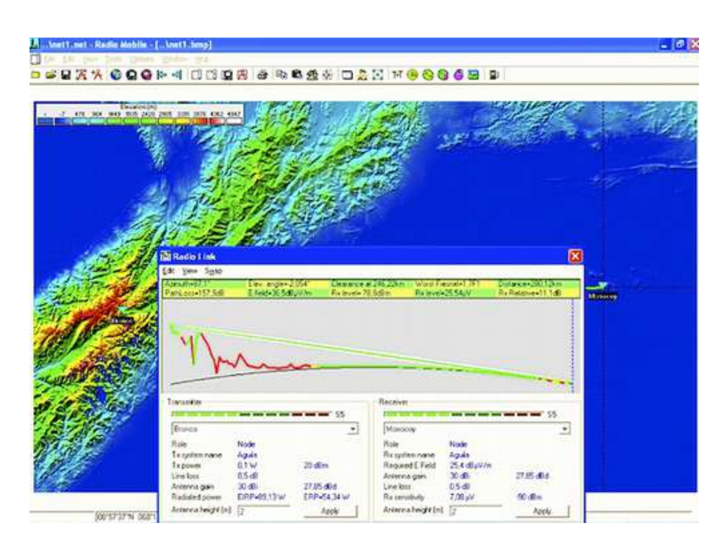


Figura IE 3: Perfi l del trayecto de 280 km sobre el cual se transmitió a 65 kb/s con equipo WiFi modificado en abril 2006, entre Pico del Águila y El Baúl, Venezuela

Nótese que la curvatura de la tierra es muy evidente y fue superada porque una de las estaciones estaba a 4100 m de altura y la otra a 155 m. La frecuencia fue de 2412 MHz, la potencia de salida de 100mW, y la ganancia de antena de 30 dBi. Se pudo transmitir video en tiempo real con éxito a pesar del ancho de banda limitado.
Un año después se repitió el experimento con el mismo equipo WiFi pero con antenas comerciales de 32 dBi en ambos extremos y se lograron resultados semejantes. Después, se experimentó con otro tipo de firmware patentado, desarrollado por el grupo TIER de la Universidad de California en Berkeley que implementa TDD (*Time Division Duplexing*) que ofreció un caudal bidireccional importante de 6 Mbits/seg con hardware de estándar 802.11b.
Al mover el sitio remoto a una colina de 1400 m de alto llamada Platillón (9.88905350°N, 67.50552400°W) se obtuvo un banco de prueba de 380 km en al cual el experimento tuvo éxito de nuevo como se describe en la sección Case Studies de este libro.

Esto puede ilustrarse usano una versión en línea de Radio Mobile disponible en http://www.cplus.org/rmw/rmonline.html, que es más sencilla de usar aunque tiene algunas limitaciones comparada con la versión descargable. Uno se registra en el sitio, entra las coordenadas de los puntos sobre los cuales se va a establecer el enlace de radio, los valores de potencia de los radios y las alturas y ganancias de las antenas, y el software le dará los datos de la elevación que se necesitan para hacer la simulación del enlace. Tome en cuenta que sólo puede usar frecuencias de radio aficionados en la versión en línea, así que debería usar 2.3 GHz en vez de 2.4 GHz, pero los resultados son bastante cercanos y se validaron mediante el experimento de campo. En la figura IE 4 mostramos la salida de Radio Mobile en línea para este experimento que puede ser replicado como ejercicio.

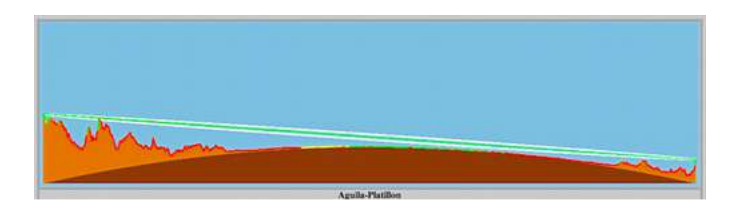


Figura IE 4: Perfil de una prueba de enlace de 380 km a 2.4 GHZ realizada en abril y agosto de 2007. Venezuela

Observe que la curvatura terrestre es aún más notable en la trayectoria de 380 km, pero la altura de los puntos extremos combinada con la tierra plana entre ellos permite un despeje amplio de la primera zona de Fresnel.

La Figura OI 5 muestra los valores numéricos de la simulación con Radio Mobile en línea:

Radio Mobile — Par/By Roger Coudé VE2DBE — Information

Latitude	8.829425 °	Latitude	9.859167 °
Longitude	-70.834667 °	Longitude	-67.521770 °
Ground elevation	4165.4 m	Ground elevation	1519.7 m
Antenna height	2.0 m	Antenna height	2.0 m
Azimuth	72.25 °	Azimuth	252.79 °
Tilt	-2.11 °	Tilt	-1.32 °
Radio system			**Propagation**
TX power	20.00 dBm	Free space loss	151.26 dB
TX line loss	0.00 dB	Obstruction loss	16.58 dB
TX antenna gain	34.00 dBi	Forest loss	1.00 dB
RX antenna gain	34.00 dBi	Urban loss	0.00 dB
RX line loss	0.00 dB	Statistical loss	2.83 dB
RX sensitivity	-97.46 dBm	Total path loss	171.67 dB

Performance	
Distance	**381.091 km**
Precision	190.6 m
Frequency	2300.000 MHz
Equivalent Isotropically Radiated Power	251.189 W
System gain	185.46 dB
Required reliability	70.000 %
Received Signal	-83.67 dBm
Received Signal	14.68 µV
Fade Margin	**13.79 dB**

Figura IE 5: Resultados de la simulación on line con Radio Mobile para el enlace de 380 km entre el Águila y Platillon, Venezuela

14. ENERGÍA AUTÓNOMA

Energía Solar

Este capítulo presenta una introducción a los componentes de un sistema fotovoltaico autónomo. La palabra autónomo (*standalone*) se refiere al hecho de que el sistema trabaja sin ninguna conexión a una red eléctrica establecida. En este capítulo se presentarán los conceptos básicos de la generación y almacenamiento de energía solar fotovoltaica. También describiremos un método para diseñar un sistema solar funcional con acceso limitado a información y recursos. Este capítulo sólo discutirá el uso de la energía solar para la producción directa de electricidad (***energía solar fotovoltaica***). La energía solar también se puede usar para calentar fluidos (***energía solar térmica***) y puede ser usada como fuente de calor o para accionar una turbina para generar electricidad. Los sistemas de energía solar térmica están fuera de los objetivos de este capítulo.

Energía solar fotovoltaica

Un sistema fotovoltaico está basado en la capacidad que tienen los paneles fotovoltaicos para convertir la radiación solar en energía eléctrica. A la cantidad total de energía solar que ilumina un área determinada se le denomina **irradianza** (***G***) y se mide en ***vatios por metro cuadrado*** (**W/m²**).

Los valores instantáneos se promedian en el tiempo y así es común hablar de irradianza total por hora, por día o por mes. La cantidad de irradianza que llega a la superficie de la tierra varía de acuerdo con las condiciones meteorológicas y depende del sitio. Por lo tanto, se hace necesario trabajar con datos estadísticos basados en la "*historia solar*" de un lugar específico. Para muchas zonas es difícil obtener información detallada, en cuyo caso hay que trabajar con valores aproximados. Existen varias organizaciones dedicadas a la producción de mapas que incluyen valores promedio de irradiación global diaria para una región. Estos valores también se conocen como ***horas de sol pico*** al día o **HSP** (**PSH** en inglés). Se puede usar el HSP de la región para simplificar los cálculos. Una unidad de "hora solar pico" corresponde a una irradiación de 1000 Vatios-hora para una hora de duración. Si encontramos que un área determinada tiene 4 HSP en el peor mes, esto quiere decir que en ese mes deberíamos esperar una irradiación diaria de 4000 Wh/m^2 por día.

Encontramos mapas de HSP de baja resolución y herramientas de cálculo en numerosos recursos en línea, tales como

http://www.wunderground.com/calculators/solar.html
Para más detalles consulte un vendedor local de energía solar o una estación meteorológica. También los aeropuertos colectan datos que incluyen la insolación.

¿Qué hay sobre la energía eólica?

Es posible usar un generador eólico en lugar de paneles solares cuando se diseña un sistema autónomo para instalar en un cerro o montaña. Para que sea efectivo, la velocidad promedio del viento en el año debería ser de por lo menos 3 a 4 metros por segundo, y el generador eólico debería colocarse a 6 metros por encima de cualquier otro objeto en un radio de 100 metros. Las ubicaciones muy alejadas de las costas carecen en general de energía suficiente para operar un sistema de energía eólico. En términos generales, los sistemas fotovoltaicos son más confiables que los generadores eólicos ya que la luz del sol es más asequible que un viento constante en la mayoría de los sitios. Como contrapartida, los generadores eólicos pueden recargar sus baterías incluso en la noche, con la condición de que haya viento suficiente. También es posible usar el viento en conjunción con energía solar para ayudar a cubrir el tiempo en que haya nubosidades persistentes o cuando haya poco viento. En Escocia, hay un proyecto que usa tanto la energía solar como la eólica para la producción de energía.
Puede verlo en: http://www.wirelesswhitespace.org/projects/wind-firenewable-energy-basestation.aspx. Sin embargo, en la mayor parte de los sitios, no se justifica el gasto de un buen generador eólico para añadir un poco de energía extra al sistema general. Este capítulo, por lo tanto, se enfocará en el uso de paneles solares para la generación de electricidad.

Componentes de un sistema fotovoltaico

Un sistema fotovoltaico básico consiste de cuatro componentes principales: el ***panel solar***, las ***baterías***, el ***regulador*** y la ***carga***. El panel genera electricidad y la batería almacena energía eléctrica. El regulador protege a la batería de las cargas y descargas excesivas. Y la carga va a ser cualquier dispositivo que necesite energía eléctrica. Es importante recordar que tanto los paneles solares como las baterías usan corriente continua (DC). Si el rango de tensión de operación de su equipo no incluye la tensión de operación de la batería será necesario utilizar algún tipo de ***convertidor***.

Si el equipo que se quiere alimentar utiliza una tensión continua diferente a la de la batería será necesario el uso de un ***convertidor DC/DC*** y si alguno de los equipos trabajan en corriente alterna necesitarás un ***convertidor DC/AC***, también conocido como ***inversor***. Todo sistema eléctrico debería también incluir varios aditamentos de seguridad para el caso de fallas, tales como interruptores termo-magnéticos (*breakers*), dispositivos protectores contra picos de tensión, fusibles, cableado de tamaño apropiado, barras de tierra, pararrayos, etc.

El panel solar

El panel solar se compone de celdas solares que colectan la radiación solar y la transforman en energía eléctrica. A esta parte del sistema se la conoce generalmente como módulo solar o generador fotovoltaico. Un banco de paneles se instala conectando un conjunto de paneles en serie y/o en paralelo a fin de proporcionar la energía necesaria para una carga específica. La corriente que da un banco de paneles varía proporcionalmente a la radiación solar. Esta variará en el tiempo debido a las condiciones climatológicas, la hora del día, la estación del año, etcétera.

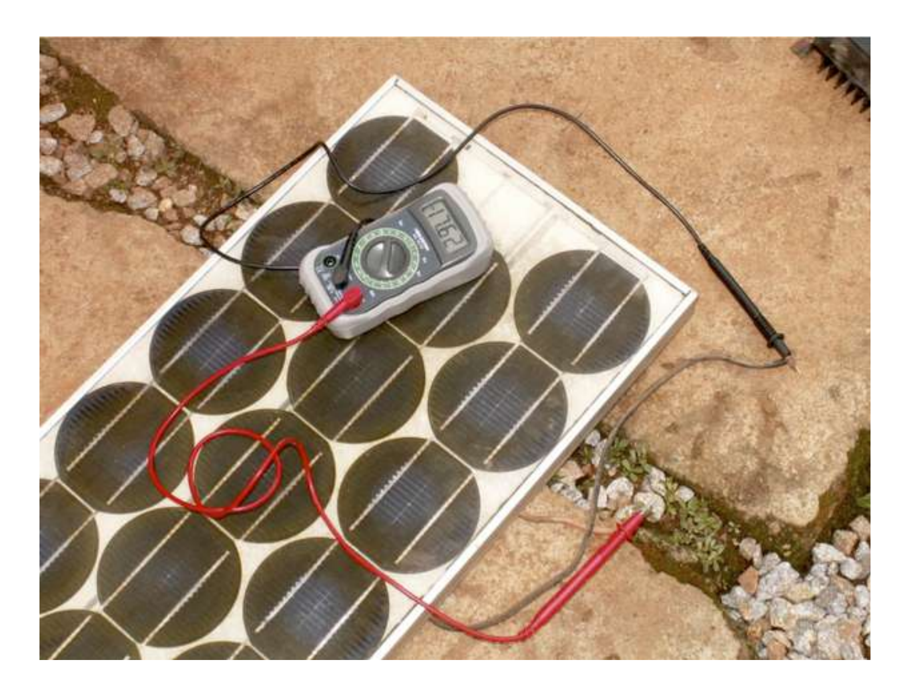


Figura EA 1: Un panel solar

Existen varias tecnologías en la manufactura de las células solares.
La más común es la de silicio cristalino, que puede ser monocristalino o policristalino. El silicio amorfo puede ser más barato pero es menos eficiente en la conversión de energía solar en electricidad. Con una expectativa de vida reducida y de un 6 a 8% de eficiencia de conversión, el silicio amorfo es comúnmente utilizado para equipos de bajo consumo de energía, como las calculadoras portátiles. Nuevas tecnologías solares como cintas de silicio y películas fotovoltaicas finas están en desarrollo en estos momentos y prometen una mayor eficiencia, pero no están muy difundidas todavía.

La batería

Almacena la energía producida por los paneles que no se consume inmediatamente para disponer de ella en periodos de baja o nula irradiación solar. Este componente es también llamado el ***acumulador***. Las baterías acumulan electricidad en forma de energía química. El tipo más común de batería empleado en aplicación solar es usualmente de plomo-ácido, también llamada recombinante o VRLA (plomo ácido, regulada por válvula, por la sigla de *valve regulated lead acid*).



Figura EA 2: Batería de plomo-ácido de 200 Ah. El terminal negativo está roto por haberle aplicado peso durante el transporte

Además de almacenar energía, las baterías de plomo-ácido también cumplen dos funciones.

- Suministrar una potencia instantánea superior a la que el banco de paneles puede generar, necesaria para la puesta en marcha de algunos elementos (por ejemplo, el motor del frigorífico o una bomba).
- Determinar el margen de tensiones de trabajo de la instalación.

Para instalaciones de baja demanda de energía y donde haya restricciones de espacio se pueden usar otros tipos de baterías tales como NiCd, NiMh, o a iones de Li. Estas, sin embargo, necesitan un cargador/regulador especial y no pueden reemplazar directamente las de plomo-ácido.

El regulador

El regulador (o más formalmente, el regulador de carga de energía solar) asegura que la batería funcione en condiciones apropiadas, evitando la sobrecarga y sobredescarga de la misma, fenómenos ambos muy perjudiciales para la vida de la batería. El procedimiento que utiliza para ello es determinar el estado de carga, SoC, (*State of Charge*) de la batería a partir de la tensión a la que ésta se encuentra. El regulador se programa en función de la tecnología de almacenamiento empleada por la batería, por lo que midiendo la tensión de la batería, determina con precisión los umbrales precisos a los que desconecta la batería para evitar la sobrecarga o descarga excesiva.



Figura EA 3: Controlador de carga solar de 30 A

El regulador puede incluir otros elementos que añaden información valiosa y control de seguridad al equipo, tales como amperímetros, voltímetros, contadores de amperios-hora, temporizadores, alarmas, etcétera. Aunque convenientes, ninguno de estos elementos se requiere para el funcionamiento del sistema fotovoltaico.

El convertidor

La electricidad proporcionada por el módulo solar y la batería es continua (DC) a un voltaje fijo. Esta tensión podría no ser la requerida por la carga que se tiene. Un convertidor continua/alterna (DC/AC en inglés) también conocido como inversor, convierte la corriente continua de la batería en corriente alterna. El precio es que se pierde algo de energía en la conversión. Si fuera necesario, se puede usar el convertidor para obtener corriente continua a niveles de tensión diferentes a los proporcionados por las baterías.
Los convertidores continua/continua también presentan pérdidas en la conversión.
Para un funcionamiento óptimo, a la hora de diseñar un sistema de comunicaciones que usa energía fotovoltaica es recomendable que todas las cargas (*loads*) trabajen a la tensión que suministran las baterías evitando el uso de convertidores.



Figura EA 4: Convertidor DC/AC. Inversor con potencia máxima de salida de 800 W

La carga

La carga está constituida por los equipos que se conectan al sistema y que consumen la energía del mismo (equipos de comunicaciones inalámbricas, enrutadores, estaciones de trabajo, iluminación, receptores de TV, módems VSAT, etc.). Aunque no es posible saber con certeza absoluta cuál va a ser el consumo total de dichos equipos en operación, es vital hacer una buena estimación del mismo ya que de esto depende la funcionalidad del sistema. Asimismo, hay que tener cuidado en elegir equipos eficientes y de bajo consumo para no derrochar energía.

Ensamblando el sistema

El sistema fotovoltaico incorpora todos estos componentes. Los paneles solares generan energía cuando se dispone de luz solar. El regulador garantiza la operación más eficiente de los paneles y previene posibles daños de las baterías. El banco de baterías almacena la energía recolectada para su uso posterior. Convertidores e inversores adaptan la energía almacenada para satisfacer las necesidades de la carga. Finalmente, la carga consume la energía almacenada para efectuar el trabajo. Cuando todos los elementos están en equilibrio y reciben mantenimiento apropiado, el sistema se soportará a sí mismo durante años.

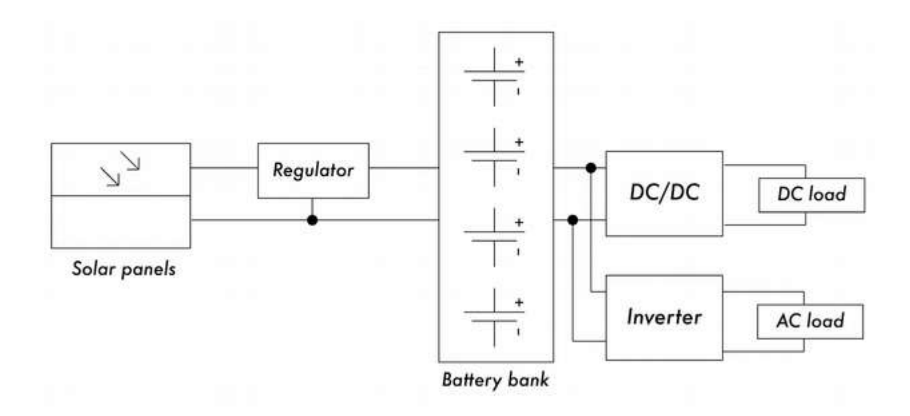


Figura EA 5: Instalación solar con cargas DC (continuas) y AC (alternas)

Examinemos ahora cada uno de los componentes individuales del sistema fotovoltaico en más detalle.

El panel solar

Un panel solar individual está compuesto de muchas celdas solares. Las celdas están conectadas eléctricamente para proporcionar un valor específico de corriente y voltaje. Las celdas individuales están debidamente encapsuladas para asegurar aislamiento y protección de la humedad y la corrosión.



Figura EA 6: Efectos del agua y la corrosión en un panel solar

Hay diferentes tipos de módulos disponibles en el mercado dependiendo de las exigencias de potencia de su aplicación. Los módulos más comunes se componen de 32 ó 36 celdas solares de silicio cristalino. Estas celdas son todas de igual tamaño, asociadas en serie y encapsuladas entre vidrio y un material plástico, con una resina polimérica (EVA) como aislante térmico. El área del módulo varía comúnmente entre 0,1 y 0,5 m^2. Los paneles solares usualmente tienen dos contactos eléctricos, uno positivo y uno negativo. Algunos paneles también incluyen contactos adicionales para permitir la instalación de ***diodos de paso*** a través de celdas individuales. Estos diodos protegen al panel contra un fenómeno conocido como "puntos calientes".

Un “punto caliente” ocurre cuando algunas celdas están a la sombra mientras que el resto del panel está a pleno sol. En lugar de producir energía, las celdas a la sombra se comportan como una carga que disipa energía. En esta situación las celdas en la sombra pueden experimentar incrementos de temperatura (unos 85 a 100°C). Los diodos de paso previenen los puntos calientes de las celdas en sombra, pero reducen el voltaje máximo del panel. Estos diodos deberían usarse sólo cuando la sombra sea inevitable. Una mejor solución es exponer completamente el panel al sol, siempre que sea posible.

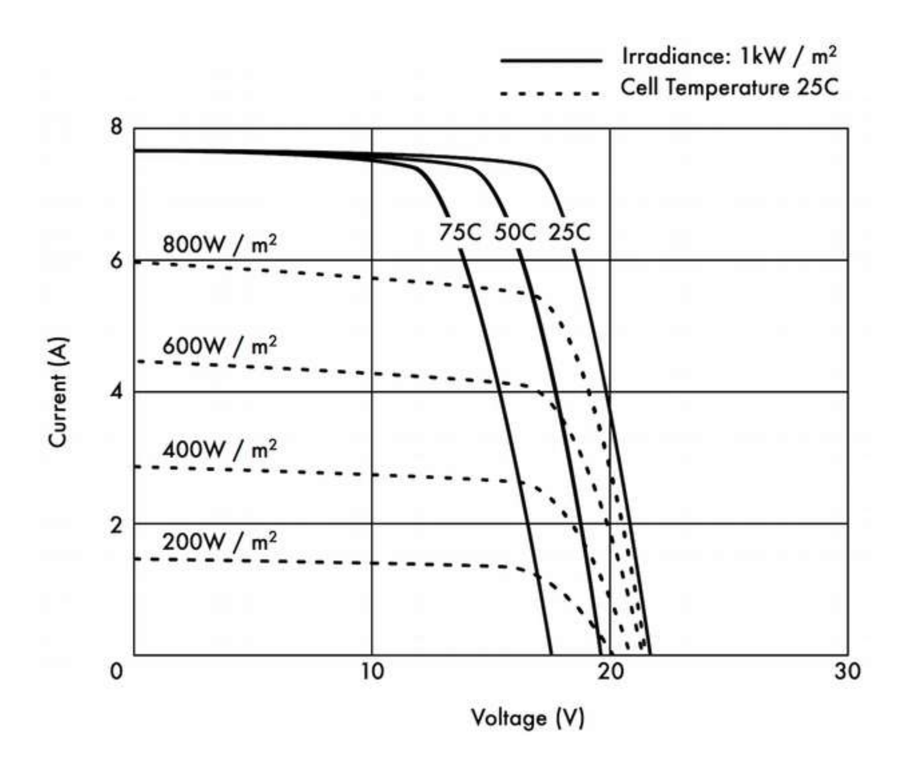


Figura EA 7: Diferentes curvas I -V. La corriente (A) cambia con la irradianza, y el voltaje (V) cambia con la temperatura

El rendimiento eléctrico de un módulo solar está representado por la **curva característica I-V**, que representa la corriente generada en función del voltaje para una radiación específica.

La curva representa todos los valores posibles de voltaje-corriente.

Las curvas dependen de dos factores principales: la temperatura y la radiación solar recibida por las celdas. Para un área de una celda solar dada, la corriente generada es directamente proporcional a la irradianza solar (G), mientras que el voltaje se reduce ligeramente con un aumento de temperatura. Un buen regulador tratará de maximizar la potencia que proporciona un panel adaptándose al punto que proporciona el valor máximo del producto de la corriente y el voltaje (V x I). La potencia máxima se corresponde con el punto de quiebre de la curva I-V.

Parámetros del Panel Solar

Los principales parámetros que caracterizan un panel fotovoltaico son:

1. **Corriente de Corto Circuito** (I_{SC}): es la máxima intensidad de corriente que proporciona el panel, y corresponde a la corriente que entrega cuando se conectan directamente los dos bornes.
2. **Tensión de Circuito Abierto** (V_{OC}): es el máximo voltaje que proporciona el panel y ocurre cuando los bornes no están conectados a ninguna carga (circuito abierto). Voc suele ser de 22 V para paneles que vayan a trabajar a 12 V, y es directamente proporcional al número de celdas asociadas en serie.
3. **Punto de Máxima Potencia** (P_{max}): el punto en el la potencia entregada por el panel es máxima, donde $P_{max} = I_{max} \times V_{max}$.

El punto de máxima potencia del panel se mide en Vatios (W) o Vatios pico (W_P). Es importante no olvidar que en condiciones normales el panel no trabajará en condiciones pico ya que el voltaje de operación está determinado por la carga o el regulador. Los valores típicos de V_{max} y de I_{max} deben ser algo menores a los de I_{SC} y V_{OC}.

4. **Factor de Forma** (FF): el factor de forma es la relación entre la potencia máxima que el panel puede entregar y el producto de $I_{SC} \times V_{OC}$. Da una idea de la calidad del panel porque es una medida de lo escarpada que es su curva característica, de forma que cuanto más se aproxima a la unidad, mayor potencia puede proporcionar. Los valores comunes suelen estar entre 0,7 y 0,8.

5. **Eficiencia (η):** es el cociente entre la máxima potencia eléctrica que el panel puede entregar a la carga y la potencia de la radiación solar (PL) que incide sobre el panel. Es habitualmente en torno al 10-12% dependiendo del tipo de celda (monocristalina, policristalina, amorfa o película delgada).

Considerando las definiciones de punto de máxima potencia y factor de forma vemos que:

$$\eta = Pmax / PL = FF . ISC . VOC / PL$$

Los valores de ISC, VOC, IPmax y VPmax son proporcionados por el fabricante y hacen referencia a las condiciones estándar de medición con valores de irradianza G = 1000 W/m2, al nivel del mar para una temperatura de las celdas de Tc = 25ºC.
Los valores de los parámetros del panel cambian para otras condiciones de irradianza y temperatura. A menudo, los fabricantes incluyen gráficos o tablas con valores ajustados a condiciones diferentes del estándar. Es aconsejable revisar los valores de rendimiento para las temperaturas del panel que más se parezcan a su instalación particular. Tenga presente que dos paneles pueden tener la misma W_p pero comportarse de manera distinta en condiciones de operación diferentes. Cuando adquiera un panel es importante verificar, en la medida de lo posible, que sus parámetros (por lo menos I_{SC} y V_{OC}) coincidan con los valores prometidos por el fabricante.

Valores del panel necesarios para el dimensionado

Para calcular el número de paneles necesario para alimentar una determinada carga, es suficiente conocer los valores de intensidad y tensión para el punto de máxima potencia: I_{Pmax} y $V_{Pmax.}$.

Usted debería recordar siempre que el panel no va a trabajar bajo condiciones ideales ya que ni la carga ni el sistema regulador van a trabajar siempre con el punto de máxima potencia del panel. Para compensar esto, se debe añadir en los cálculos una pérdida de eficiencia del 5%.

Interconexión de los paneles

Un ***banco de paneles solares*** es un conjunto de paneles solares que están interconectados eléctricamente e instalados en algún tipo de estructura de soporte.

El uso de un banco de paneles le va a permitir generar una tensión o una corriente superiores a la que se genera con un solo panel. Los paneles están interconectados de manera que la tensión generada es próxima (pero mayor) que la tensión de las baterías, y la corriente producida es suficiente para alimentar el equipo y para cargar las baterías. Conectar los paneles en serie aumenta la tensión generada mientras que conectarlos en paralelo incrementa la corriente. El número de paneles usados debería incrementarse hasta que la cantidad de energía generada exceda ligeramente las demandas de su carga. Es muy importante que todos los paneles de su banco sean lo más semejante posible, de la misma marca y características, ya que cualquier diferencia en sus condiciones operativas afectarán en gran medida las condiciones y el desempeño de su sistema. Incluso paneles que tienen un desempeño idéntico van a presentar alguna variación en sus características debido a diferencias en el proceso de fabricación. Cuando le sea posible, es buena idea probar el desempeño real de los paneles individuales para verificar sus características operativas antes de ensamblarlas en un banco de paneles.

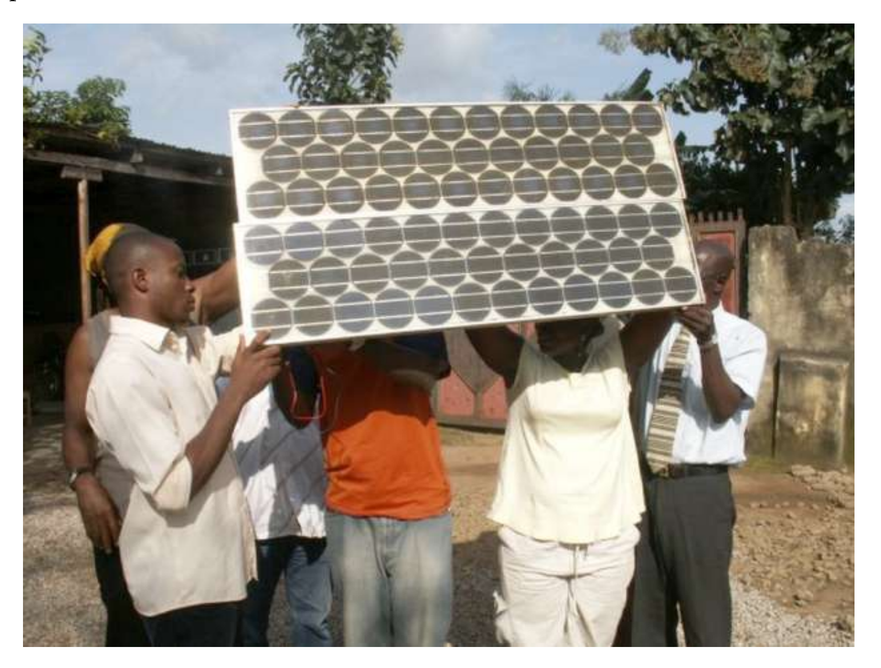


Figura EA 8: Interconexión de paneles en paralelo. La tensión permanece constante mientras que la corriente se duplica. (Foto: Fundación Fantsuam, Nigeria)

Para seleccionar un buen panel

Una medida obvia cuando se compran paneles es comparar la relación entre el punto de máxima potencia nominal (W_p) y el precio. Esto le dará una idea aproximada del costo por vatios de los diferentes paneles. Pero hay otras consideraciones que también deberían tomarse en cuenta. Si usted va a instalar paneles solares en áreas geográficas donde la suciedad (causada por arena, polvo, cascajo) puede ser un problema; considere entonces la compra de paneles que repelan el polvo. Estos paneles se fabrican con materiales que favorecen la limpieza automática con ayuda del viento o la lluvia. Revise siempre la construcción mecánica de cada panel. Verifique que el vidrio sea resistente y el marco de aluminio robusto y bien construido. Las celdas solares dentro del panel pueden durar más de 20 años, pero son muy frágiles y se debe proteger el panel de accidentes mecánicos. Examine las garantías del fabricante respecto a la potencia que deben suministrar y a la construcción mecánica.

Finalmente, asegúrese de que el fabricante le proporciones no sólo el punto de máxima potencia nominal del panel (W_p), sino también la variación de la tensión con la irrradiación y la temperatura. Esto es particularmente importante cuando los paneles se usan en bancos, ya que las variaciones en los parámetros operativos afectan grandemente la calidad de la energía generada y la vida útil de los paneles.

La batería

La batería "alberga" una reacción química reversible que hace posible el almacenamiento de energía para ser recuperada posteriormente cuando se necesite. La energía eléctrica se transforma en química cuando la batería se carga, y lo opuesto sucede cuando se descarga. Una batería está conformada por una serie de elementos llamados celdas dispuestas en serie. Una batería de plomo-ácido consta de dos electrodos de plomo inmersos en una solución electrolítica de agua y ácido sulfúrico. Una diferencia de potencial de unos 2 voltios se establece entre los electrodos dependiendo del estado de carga de la batería.

Las baterías más comunes en aplicaciones solares fotovoltaicas tienen un voltaje nominal de 12 ó 24 voltios. Por lo tanto, una batería de 12 V contiene 6 celdas en serie.

La batería tiene dos propósitos fundamentales en un sistema fotovoltaico:

proporcionar energía eléctrica al sistema cuando el banco de paneles no la proporciona, y almacenar la energía proporcionada por los paneles cuando aquella excede las necesidades de la carga. La batería pasa por ciclos de carga y descarga dependiendo de la presencia o ausencia de luz solar.

Durante las horas de sol, el banco de paneles produce energía eléctrica. La energía que no es consumida de inmediato se usa para cargar la batería. Durante las horas sin sol, cualquier necesidad de energía es provista por la batería, por lo tanto, se produce su descarga. Estos ciclos de carga y descarga ocurren cada vez que la energía producida por los paneles no satisface la cantidad de energía necesaria para alimentar la carga. Cuando hay luz suficiente y la carga es ligera, las baterías se cargarán.

Obviamente, en la noche se descargarán a la menor demanda de energía. También se descargarán cuando la radiación es insuficiente para satisfacer los requisitos de la carga (debido a variaciones climatológicas naturales tales como nubes, polvo, etc.).

Si la batería no almacena energía suficiente para satisfacer la demanda durante los períodos sin sol, no habrá energía disponible. Por otra parte, el sobre-dimensionamiento del sistema (por la adición de demasiados paneles o baterías) resulta caro e improductivo.

Cuando se diseña un sistema autónomo tenemos que llegar a un compromiso entre el costo de los elementos y la disponibilidad de energía en el sistema. Una forma de hacerlo es calcular el número de días de autonomía necesarios. En el caso de un sistema de telecomunicaciones, el número de días de autonomía dependerá de lo crítico de su función dentro de la red que se haya diseñado. Si el sistema solar va a funcionar de servidor y es parte de la troncal de su red, debe diseñar su sistema fotovoltaico con una autonomía de 5 a 7 días. Por otra parte, si el sistema solar va a encargarse de proporcionar energía a un equipo cliente, probablemente se puede reducir los días de autonomía a 2 ó 3. En áreas de baja irradiación, este valor debería incrementarse aún más. De cualquier manera, siempre tendrá que encontrar un equilibrio entre costo y disponibilidad.

Tipos de batería

Hay diferentes tipos de tecnología para baterías dependiendo de los diferentes usos de estas. La más conveniente para aplicaciones fotovoltaicas es la llamada **batería estacionaria,** diseñada para tener un emplazamiento fijo y para sitios donde el consumo de energía es más o menos irregular. Las

baterías "estacionarias" pueden permitir ciclos de descarga profunda, pero no están diseñadas para producir corrientes altas en períodos cortos de tiempo.
Las baterías estacionarias pueden usar un electrolito alcalino (como las de Níquel-Cadmio), o ácido, (como las de Plomo-ácido). Las baterías estacionarias basadas en Níquel-Cadmio se recomiendan, cuando sea posible, por su alta confiabilidad y resistencia. Desafortunadamente suelen ser mucho más caras y difíciles de conseguir que las selladas de Plomo-ácido. En muchos casos cuando se hace difícil conseguir localmente baterías estacionarias buenas y baratas (importarlas no es barato), se verá forzado a usar baterías diseñadas para automóviles.

Uso de baterías para automóviles

Las baterías de automóvil no son muy apropiadas para aplicaciones fotovoltaicas porque están diseñadas para proporcionar intensidades elevadas durante unos cuantos segundos (al encender el auto) en vez de mantener intensidades bajas por largos períodos. Este diseño característico de baterías de automóvil (también llamadas **baterías de tracción**) se traduce en un acortamiento de su vida útil cuando se usa para sistemas fotovoltaicos. Las baterías de tracción pueden usarse en pequeñas aplicaciones cuando el bajo costo sea la consideración más importante o cuando no se encuentre otro tipo de baterías.

Las baterías de tracción están diseñadas para vehículos y montacargas eléctricos. Son más baratas que las estacionarias y pueden usarse en sistemas fotovoltaicos, pero hay que tomar en cuenta que necesitan mantenimiento frecuente. Estas baterías no deben descargarse profundamente porque se reduce notablemente su capacidad de cargarse. Una batería de camión no debería descargarse más del 70% de su capacidad total. Esto significa que se puede usar un máximo de 30% de la capacidad nominal de una batería plomo-ácido antes de ser cargada de nuevo.

Se puede extender la vida de una batería plomo-ácido utilizando agua destilada. Al usar un densímetro o un hidrómetro se puede medir la densidad del electrolito de la batería.

Una batería típica tiene una densidad específica de 1,28. Al añadir agua destilada, y bajar la densidad a 1,2, se puede reducir la corrosión del ánodo a expensas de la capacidad total de la batería. Si usted ajusta la densidad del electrolito de la batería, debe usar agua destilada, porque el agua de grifo o de pozo la dañará permanentemente.

Estados de carga

Hay dos estados especiales de carga que pueden ocurrir durante las cargas y descargas cíclicas de la batería. Ambos deberían evitarse para preservar la vida útil de la batería.

1. **Sobrecarga**

La **sobrecarga** ocurre cuando la batería llega al límite de su capacidad. Si se sigue inyectando energía a la batería más allá de su punto de carga máxima, el electrolito comienza a descomponerse. Esto produce burbujas de oxígeno e hidrógeno en un proceso que se llama **gasificación**. Los resultados son pérdida de agua, oxidación en el electrodo positivo y, en casos extremos, hay riesgos de explosión. Por otra parte, la presencia de gas evita la estratificación del ácido. Después de continuos ciclos de carga y descarga, el ácido tiende a concentrarse en el fondo de la batería con lo que se reduce su capacidad efectiva. El proceso de gasificación, entonces, revuelve el electrolito y evita la estratificación.

De nuevo, es necesario encontrar un compromiso entre las ventajas (evitar la estratificación electrolítica) y las desventajas (pérdida de agua y producción de hidrógeno). Una solución es la de permitir una ligera sobrecarga de vez en cuando. El método más común es permitir una tensión de 2,35 a 2,4 voltios por cada elemento de la batería a 25°C, cada pocos días. El regulador debería asegurar sobrecargas periódicas y controladas.

2. **Sobredescarga**

De la misma manera en que hay un límite superior, también hay un límite inferior respecto a la carga de una batería. Descargarla por debajo del límite inferior puede significar el deterioro de la batería. Cuando la energía efectiva de la batería se consume, el regulador se encarga de que no se siga extrayendo energía de la batería. Cuando la tensión alcanza un límite mínimo de 1,85 voltios por celda a 25°C , el regulador desconecta la carga de la batería. Si la descarga es muy profunda y la batería permanece mucho tiempo descargada, pueden ocurrir tres cosas: la formación de sulfato cristalizado en las placas de la batería, el aflojamiento del material activo de las placas de la batería, o la deformación de las placas. Al proceso de formación de cristales permanentes de sulfato se le conoce como sulfatación, lo que es particularmente perjudicial, ya que se generan grandes cristales que no forman parte de ninguna reacción química y que pueden dañar la batería de manera irreversible.

Parámetros de la batería

Los principales parámetros que caracterizan a una batería son:

Tensión Nominal, V_{NBat}: el valor más común es 12 V.

Capacidad Nominal, C_{NBat}: Cantidad máxima de energía que se puede extraer de una batería con carga completa. Se expresa en amperios-hora (Ah) o vatios-hora (Wh). La cantidad de energía que se puede extraer de una batería depende del tiempo en que se efectúe el proceso de extracción. Descargar una batería durante un periodo largo nos proporciona más energía que descargar la misma batería por corto tiempo. Por lo tanto, la capacidad de una batería se especifica a diferentes tiempos de descarga. Para aplicaciones fotovoltaicas este tiempo debe ser de 100 horas o más (C100).

Profundidad Máxima de Descarga, DoDmax: La profundidad de descarga es la cantidad de energía extraída de una batería en un ciclo único de descarga, expresada como porcentaje. La esperanza de vida de una batería depende de la profundidad de su descarga en cada ciclo. El fabricante debería proporcionar gráficos que muestre la relación entre el número de ciclos de carga-descarga y la vida de la batería. Como regla general, para baterías de ciclo profundo, deberían evitarse descargas mayores al 50%, y para las de uso automotriz, mayores al 30%.

Capacidad Útil, CUBat: Es la capacidad real (disponible) de una batería. Es igual al producto de la capacidad nominal por la profundidad máxima de descarga DoDmax. Por ejemplo, una batería estacionaria de capacidad nominal con tiempo de descarga de 100 horas (C100), de 120 Ah y profundidad de descarga de 70%, tiene una capacidad útil de (120 x 0,7) = 84 Ah.

Medida del estado de carga de la batería

Una batería de plomo-ácido de 12 V entrega diferente voltaje a los equipos dependiendo del estado de su carga. Cuando la batería está cargada al 100%, el voltaje de salida en circuito abierto es de 12.8 V y baja rápidamente a 12.6 V cuando se le conectan las cargas.

Debido a que la batería tiene que entregar una corriente constante cuando está en operación, el voltaje de la batería baja linealmente a 12.6 dependiendo del estado de carga. Las baterías de plomo-ácido entregan el 95% de su energía dentro de este margen.

Si estimamos que una batería está al 100% con 12.6 V y vacía (0%) con 11.6 V, podemos estimar que el voltaje, cuando la batería se ha descargado un 70%, es de 11.9 V. Estos valores son sólo una aproximación basta, ya que van a depender de la vida de la batería, la temperatura y calidad de la misma, etc.

Estado de carga	12V Voltaje de la batería	Voltaje por Celda
100%	12.07	2.12
90%	12,5	2.08
80%	12.42	2.07
70%	12.32	2.05
60%	12.2	2.03
50%	12.06	2.01
40%	11.9	1.98
30%	11.75	1.96
20%	11.58	1.93
10%	11.31	1.89

De acuerdo con esta tabla, y considerando que una batería de camión no debería descargarse más del 20 ó 30%, podemos determinar que la capacidad útil de una batería de camión de 170 Ah es de 34 Ah (20%) a 51 Ah (30%). Usando la misma tabla, encontramos que deberíamos programar el regulador para que impida la descarga de la batería por debajo de 12. 3 V.

Protección de la batería y el regulador

Para proteger las baterías y las instalaciones de cortocircuitos y fallas se usan corta-circuitos termomagnéticos y fusibles. Hay dos tipos de fusibles, de **fusión lenta** y de **fusión rápida.** Deberían de usarse de fusión lenta con cargas inductivas y capacitivas donde pueden ocurrir corrientes muy altas en el momento de encender el aparato. Los fusibles de fusión lenta permiten que corrientes más altas que las estipuladas pasen por un corto tiempo. Los fusibles de difusión rápida, en estos mismos casos, se fundirían rápidamente. El regulador se conecta a la batería y a las cargas de manera que se deben considerar dos tipos diferentes de protección.

Un fusible debería colocarse entre la batería y el regulador para proteger la batería de cortocircuitos, en caso de que el regulador falle. Un segundo fusible es necesario para proteger el regulador de una excesiva corriente absorbida por la carga. Este segundo fusible está normalmente integrado al mismo regulador.



Figura EA 9: Un banco de baterías de 3.600 Ah. La corriente alcanza niveles de 45 A durante la carga

Cada fusible tiene estipulados una corriente máxima y un voltaje máximo de uso. La corriente máxima del fusible debería ser 20% más grande que la corriente máxima esperada. Aunque las baterías tienen un voltaje bajo, un cortocircuito puede ocasionar corrientes altas que pueden fácilmente alcanzar varios cientos de amperios. Las corrientes altas pueden ocasionar fuego, dañar los equipos y baterías e incluso causar quemaduras al cuerpo humano. Si un fusible se funde, nunca lo reemplace con un alambre o un fusible estipulado para corrientes más altas sino que, en primer lugar, determine la causa del problema, y luego sustituya el fusible con otro que tenga las mismas características.

Efectos de la temperatura

La temperatura ambiente tiene algunos efectos importantes en la características de una batería:

- La capacidad nominal de una batería (que el fabricante suele dar para 25°C) aumenta con la temperatura a razón de un 1%/°C, aproximadamente. Pero en el caso de que la temperatura sea demasiado alta, la reacción química que tiene lugar en la batería se acelera, lo que puede provocar la oxidación mencionada al hablar de la sobrecarga. Esto, naturalmente, reducirá la vida de la batería. Para baterías automotrices, este problema se compensa en parte utilizando densidades de solución bajas (de gravedad específica de 1,25 cuando la batería está totalmente cargada).

- A medida que la temperatura se reduce, la vida útil de la batería aumenta, pero si la temperatura es demasiado baja se corre el riesgo de congelar el electrolito. La temperatura de congelación depende de la densidad de la solución, a su vez directamente relacionada con el estado de carga de la batería. A menor densidad, mayor el riesgo de congelamiento. En zonas de temperatura baja debería evitarse las descargas profundas de la batería (es decir, DoDmax efectivamente reducido).

- La temperatura también cambia la relación entre el voltaje y la carga. Es preferible usar un regulador que ajuste los valores de desconexión y reconexión por bajo voltaje de acuerdo con la temperatura. El sensor de temperatura del regulador debería estar fijado a la batería con cinta pegante o por otro medio sencillo.

- En zonas calientes es importante mantener las baterías tan frías como sea posible. Deben almacenarse en áreas sombreadas y nunca exponerse directamente al sol. También se aconseja colocarlas sobre un soporte pequeño para permitir que el aire fluya por debajo y, de esta manera, aumentar el enfriado.

Cómo escoger una buena batería

Escoger una buena batería conlleva decisiones difíciles.
Las baterías de gran capacidad son pesadas, voluminosas y caras de importar.
Una batería de 200 Ah pesa unos 50 kg y no puede ser transportada como equipaje de mano. Si quiere una batería duradera (5 o más años) y sin mantenimiento hay que pagar un precio.
Una buena batería debe traer siempre especificaciones técnicas, incluso la capacidad a diferentes tasa de descarga(C20, C100), temperatura de operación, valores críticos de voltaje y especificaciones para los cargadores.

La batería no debe presentar rajaduras, derrame de líquidos u otra señal de daño y sus bornes deben estar libres de corrosión.

Puesto que para tener datos confiables sobre las baterías se necesitarían pruebas de laboratorio sobre capacidad real y envejecimientos, hay que estar alerta si nos ofrecen baterías de baja calidad (y hasta falsificaciones) en el mercado local.
Un precio normal (sin incluir transporte o impuestos de importación) es de 3-4 US $ por Ah para las baterías de plomo-ácido.

Esperanza de vida versus número de ciclos

Las baterías son el único componente en un sistema fotovoltaico que se debería amortizar en un corto periodo y que debería reemplazarse a menudo.
Se puede aumentar la vida útil de una batería reduciendo la profundidad de descarga por ciclo. Incluso las baterías de ciclo profundo obtendrán un aumento en su duración si el número de ciclos de descargas profundas (> 30%) se reduce.
Si descarga completamente la batería a diario es probable que necesite cambiarla en poco menos de un año. Si usa sólo 1/3 de la capacidad de la batería, puede durarle más de tres años.
Puede que sea más barato comprar una batería con el triple de capacidad que cambiarla cada año.

El regulador de carga

El regulador de carga se conoce también como controlador de carga,

regulador de voltaje, controlador de carga-descarga, o controlador de carga-descarga y controlador de la carga (*load*). El regulador se posiciona entre el banco de paneles, la batería y el equipo o carga.

Recuerde que el voltaje de una batería, a pesar de que es cercano a 2V por celda, varía de acuerdo con su estado de carga. El regulador impide las sobrecargas o sobredescargas monitoreando el voltaje de la batería. Los reguladores que se usan en sistemas fotovoltaicos deben conectarse en serie; así desconectan el banco de paneles del banco de baterías para evitar la sobrecarga, y desconectan las baterías de la carga para evitar la sobredescarga. La conexión y desconexión se efectúa por medio de interruptores que pueden ser de dos tipos: electromecánicos (relés) o de estado sólido (transistor bipolar, MOSFET). Los reguladores nunca deben conectarse en paralelo. Para proteger la batería de la gasificación, el interruptor se abre cuando la tensión en la batería alcanza su tensión de corte alta (*high voltage disconnect*, HVD). La tensión de corte baja (*low voltage disconnect*, LVD) impide que la batería se sobredescargue por medio de la desconexión de la carga. Para impedir las continuas conexiones y desconexiones, el regulador no se reconectará hasta que la batería alcance su tensión de rearme por baja (*low reconnect voltage* LRV).

Los valores característicos de una batería plomo-ácido de 12 V son:

Umbrales de voltaje	Voltaje
LVD	11.5
LRV	12.6
Voltaje Regulado Constante	14.3
Ecualización	14.6
HVD	15.5

Los reguladores más modernos son también capaces de desconectar automáticamente los paneles durante la noche para evitar la descarga de la batería. Pueden también sobrecargarla cada cierto tiempo para incrementar su vida, y usar un mecanismo conocido como modulación de duración de impulsos (*pulse width modulation*, PWM) para prevenir la gasificación excesiva. Como el punto de operación de máxima potencia del banco de paneles va a variar con la temperatura y la iluminación solar, los reguladores modernos son capaces de rastrear el punto de potencia máxima del banco

de paneles solares. Esta característica se conoce como rastreo del punto de máxima potencia (*maximum power point tracking*, MPPT).

Parámetros del regulador

Cuando seleccione un regulador para su sistema, debería conocer, al menos, la **tensión de trabajo** y la **máxima corriente** que aquel puede manejar. La tensión de trabajo será de 12, 24 ó 48 V. La máxima corriente debe ser 20% más grande que la proporcionada por los paneles conectados al regulador.

Otras características y datos de interés son:

- Valores específicos de tensión de corte por baja (LVD), tensión de rearme por baja (LRV) y tensión de corte por alta (HVD).
- Compensación por temperatura. Las tensiones que indican el estado de carga de la batería varían con la temperatura. Por esta razón, algunos reguladores pueden medir la temperatura de la batería y corregir las tensiones de sobrecarga.
- Instrumentación e indicadores. Los instrumentos más comunes miden la tensión de los paneles y las baterías, el estado de carga (SoC) o Profundidad de Descarga (DoD). Algunos reguladores incluyen alarmas especiales que indican que el panel o la carga han sido desconectados, que se ha alcanzado la LVD o HVD, etc.

Convertidores

El regulador proporciona potencia a un voltaje continuo específico. Los convertidores e inversores se usan para ajustar el voltaje a las necesidades de la carga.

Convertidores DC/DC

Los convertidores DC/DC transforman un voltaje continuo en otro también continuo de valor diferente. Hay dos métodos de conversión que se usan para adaptar el voltaje al de las baterías: *conversión lineal* y *conversión conmutada*. La conversión lineal baja el voltaje de las baterías por conversión del exceso de energía en calor.

Este método es muy simple, pero obviamente ineficiente. La conversión conmutada usa generalmente un componente magnético para almacenar temporalmente la energía y transformarla en otro voltaje que puede ser

mayor, menor o el inverso (negativo) del voltaje de entrada. La eficiencia de un regulador lineal disminuye a medida que se incrementa la diferencia entre el voltaje de entrada y el de salida. Por ejemplo, si queremos convertir de 12 V a 6 V, el regulador lineal tendrá una eficiencia de sólo el 50%. Un regulador de conmutación tiene una eficiencia de, por lo menos, un 80%.

Convertidor o inversor de continua a alterna (DC/AC)

Los inversores se usan cuando su equipo requiere de corriente alterna. Los inversores cortan e invierten la corriente continua y generan una onda cuadrada que es luego filtrada para aproximarla a una onda sinusoidal y eliminar los armónicos indeseables. Muy pocos inversores proporcionan una sinusoidal pura como salida. La mayoría de los modelos disponibles en el mercado producen lo que se llama "onda sinusoidal modificada", ya que el voltaje de salida no es una sinusoidal pura. En términos de eficiencia, los inversores de onda modificada trabajan mejor que los de onda sinusoidal pura. Tenga presente que no todos los equipos aceptarán una onda sinusoidal modificada como voltaje de entrada. Muy frecuentemente las impresoras láser no trabajan con inversores de onda modificada. Los motores sí trabajan, pero podrían consumir más energía que si trabajaran con sinusoidal pura. Además, las fuentes de alimentación de corriente continua (DC) tienden a calentarse más, y los amplificadores de audio a veces emiten un zumbido en presencia de inversores de onda sinusoidal modificada. Aparte de la forma de onda, algunas características importantes que deben tener los inversores son:

Confiabilidad ante sobrecorrientes. Los inversores tienen dos especificaciones de potencia: una para la potencia promedio y otra para la potencia máxima. Son capaces de proporcionar la potencia máxima por breve tiempo, como cuando se enciende un motor. El inversor debería también ser capaz de autointerrumpirse de manera segura (con un cortacircuito o un fusible) en la eventualidad de un cortocircuito, o si la potencia requerida fuera muy alta.

Eficiencia de conversión. Los inversores presentan su máxima eficiencia cuando proporcionan del 50% al 90% de su especificación de potencia promedio. Usted debería seleccionar el inversor que satisfaga lo más posible las demandas de la carga. El fabricante normalmente proporciona el rendimiento del inversor al 70% de su potencia nominal.

Cargador de batería. Muchos inversores también incorporan la función inversa: la posibilidad de cargar baterías en presencia de una fuente alternativa de energía (red eléctrica, generador, etc.). Este tipo de inversor se conoce como cargador/inversor.

Conmutación automática. Algunos inversores pueden conmutar automáticamente entre diferentes fuentes de energía (red eléctrica, generador, solar) dependiendo de lo que esté disponible.

Cuando se usan equipos de telecomunicaciones es mejor evitar el uso de convertidores de continua a alterna (DC/AC); es mejor alimentarlos directamente con tensión continua. La mayoría de los equipos de telecomunicaciones aceptan un rango amplio de voltaje de entrada.

Equipo o carga

Obviamente, a medida que hay mayor demanda de consumo, el costo del sistema fotovoltaico también aumenta. Es, esencial, entonces, dimensionar el sistema adecuándolo lo más posible al consumo esperado. Cuando diseñe el sistema, debe hacer un estimado realista del consumo máximo, y una vez que el sistema esté instalado, el consumo máximo establecido debe respetarse para evitar fallas frecuentes de energía.

Equipos domésticos

No se recomienda el uso de energía solar fotovoltaica para aplicaciones de intercambio de calor (calentadores eléctricos, refrigeradores, tostadoras, etc.). Cuando le sea posible la energía debe ser usada con moderación utilizando aparatos de bajo consumo.

A continuación enumeramos algunos puntos que se deben considerar cuando escoja equipos apropiados para usar con un sistema de energía solar:

- La energía solar fotovoltaica es adecuada para iluminación. En este caso, el uso de lámparas halógenas o fluorescentes es obligatorio ya que, aunque más caras, tienen más rendimiento que las bombillas incandescentes. Las lámparas a diodos emisores de luz (LED) también son una buena elección, ya que dan un buen rendimiento y se alimentan con corriente continua.
- También es posible usar energía fotovoltaica para aplicaciones que requieren consumo bajo y constante (el ejemplo más común es el televisor). Los televisores más

pequeños consumen menos energía que los grandes. También debe considerarse que un televisor en blanco y negro consume cerca de la mitad de la energía de uno a color.

- La energía solar fotovoltaica tampoco se recomienda en el caso de aplicaciones que transforman la energía en calor (energía térmica). Se recomienda en su lugar el uso de calentadores solares o de butano.
- Las lavadoras de ropa automáticas convencionales pueden usarse, pero debe evitarse usar programas de centrifugado o calentamiento de agua.
- Si debe usar un refrigerador, debería ser de bajo consumo. Hay algunos especiales que trabajan con corriente continua, sin embargo su consumo es bastante alto (cerca de 1.000 Wh / día).

La estimación del consumo total es un paso fundamental en el cálculo de su sistema de energía solar.
A continuación encontrará una tabla que le da una idea general del consumo de energía que se puede esperar con diferentes equipos.

Equipo	Consumo (Vatios)
Computadora portátil	30-50
Lámpara de baja potencia	6-10
Enrutador, WRAP (un radio)	4-10
Módem VSAT	15-30
PC de bajo consumo (sin LCD)	20-30
PC con LCD	200-300
Switch Ethernet (16 puertos)	6-8

Equipo de telecomunicaciones inalámbricas

Ahorrar energía al seleccionar el equipo adecuado le puede ahorrar bastante dinero y problemas. Por ejemplo, un enlace de larga distancia no necesita necesariamente un amplificador fuerte que consuma grandes cantidades de

potencia. Una tarjeta WiFi con buena sensibilidad de receptor y con la zona de Fresnel despejada por lo menos en un 60%, trabajará mejor que un amplificador y también le ahorrará consumo.

Un dicho popular entre los radioaficionados se puede aplicar aquí también: el mejor amplificador es una buena antena. Algunas medidas adicionales para el ahorro de energía incluyen limitar la velocidad del CPU, reduciendo la transmisión de energía al mínimo necesario para permitirle estabilidad al enlace, incrementando el intervalo entre balizas (*beacons*), y apagando el sistema cuando no se necesite.

La mayor parte de los sistemas solares autónomos trabajan a 12 ó 24 voltios. Es preferible usar un dispositivo inalámbrico que funcione con corriente continua trabajando a los 12 voltios que la mayoría de las baterías plomo-ácido proporciona.

Cuando se transforma el voltaje proporcionado por la batería en corriente alterna, o cuando se usa un voltaje a la entrada del Punto de Acceso (*Access Point, AP*) diferente al voltaje de la batería, se ocasionará una pérdida innecesaria de energía. Un enrutador, o un AP que acepte 8-20 voltios DC, sería perfecto.

La mayoría de los AP baratos traen incorporado un regulador de voltaje tipo conmutado y trabajarán en rangos amplios de voltaje, sin modificaciones y sin recalentarse (incluso si el dispositivo viene con una fuente de alimentación de 5 ó 12 voltios).

ADVERTENCIA: Cuando opere su AP con una fuente de alimentación diferente a la que provee el fabricante, cualquier garantía quedará anulada y puede dañar su equipo. Aunque la técnica siguiente va seguramente a funcionar como se describe, recuerde, que si la utiliza, lo hace a su propio riesgo.

Abra su AP y busque cerca de la entrada DC dos capacitores (condensadores) relativamente grandes y un inductor (un toroide de ferrita con un alambre de cobre enrollado alrededor). Si los encuentra, es porque el dispositivo tiene una entrada tipo conmutada, y el voltaje máximo de entrada debería ser un poco menor que el voltaje especificado en los capacitores. Esta especificación es, normalmente, 16 ó 25 voltios.
Tenga en cuenta que una fuente de alimentación no regulada tiene un rizado y podría aplicar un voltaje mucho más alto a su AP que el especificado. Por lo tanto, conectar una fuente de alimentación no regulada

de 24 voltios a un dispositivo con un condensador de 25 voltios no es una buena idea.
Naturalmente, cuando usted abre su dispositivo, pierde cualquier garantía. Así que no trate de operar un AP a un voltaje más alto si no tiene un regulador tipo conmutado porque se calentará, presentará fallas o se quemará.
Los equipos basados en CPU Intel x86 tradicionales son grandes consumidores de energía comparados con arquitecturas basadas en RISC, tales como ARM o MIPS.

Una de las placas con menor consumo de energía es la plataforma Soekris que usa un procesador AMD Elan SC520. Otra alternativa a AMD (Elan SC ó Geode SC1100) es el uso de equipo con procesadores MIPS. Estos procesadores presentan mejor rendimiento que un AMD Geode al precio de consumir entre 20 y 30% más de energía.

La cantidad de potencia que requiere un equipo inalámbrico depende no sólo de la arquitectura sino del número de interfaces de red, radios, tipo de memoria/almacenamiento y del tráfico. Por regla general, una tarjeta inalámbrica de bajo consumo, usa de 2 a 3 W, y una tarjeta de radio de 200mW disipa unos 3 W. Las tarjetas de alta potencia (como la Ubiquiti 400 mW) consumen alrededor de 6 W, y una estación repetidora con dos radios está en el rango de los 8 a 10 W.

A pesar de que el estándar IEEE 802.11 incorpora un mecanismo de ahorro de energía (PS), los beneficios no son tan buenos como se pudiera esperar. El principal mecanismo de ahorro de energía es permitirle a las estaciones que periódicamente "pongan a dormir" sus tarjetas por medio de un circuito temporizador.
Cuando la tarjeta inalámbrica "despierta", verifica si hay alguna baliza (*beacon*) lo que indica tráfico pendiente tráfico pendiente para ella. El ahorro de energía, entonces, sólo se efectúa en la parte del cliente, ya que el AP siempre necesita estar despierto para enviar balizas y almacenar el tráfico de los clientes.
El modo de ahorro de energía podría ser incompatible entre las implementaciones de diferentes fabricantes, lo que podría ocasionar inestabilidad a las conexiones inalámbricas. Es casi preferible desactivar siempre el modo de ahorro de energía en todos los equipos ya que los problemas que ocasionan son más importantes que la energía que se ahorra.

Selección del voltaje de trabajo

La mayoría de los sistemas autónomos de bajo consumo usan 12 V que es el voltaje de trabajo más común en baterías de plomo-ácido. Cuando diseñe un sistema inalámbrico necesita tomar en cuenta el voltaje de trabajo más eficiente para su equipo. Aunque el equipo pueda aceptar un rango amplio de valores de voltaje, escoja el que le permita que el consumo total del sistema sea mínimo.

Cableado

Este es un aspecto importante de su instalación ya que un cableado adecuado le va a asegurar una transferencia eficiente de energía. Algunos buenos hábitos que debería recordar en esta sección son:

- Use un tornillo para asegurar el cable al borne de la batería. Las conexiones flojas ocasionan pérdidas de energía.
- Unte vaselina o jalea mineral en los bornes de la batería. La corrosión en las conexiones ocasiona aumento en la resistencia, es decir, gasto de energía.

El tamaño de los cables normalmente se encuentra en American Wire Gauge (AWG).

Para sus cálculos, necesita convertir de AWG a mm^2 para calcular la resistencia del cable. Por ejemplo, un cable AWG # 6 tiene un diámetro de 4,11 mm y puede manejar hasta 55 A.
En el **Apéndice D: Tamaño de los Cables** va a encontrar una **tabla de conversión** que incluye un estimado de resistencia y de capacidad de transporte de corriente.
Tenga en cuenta que la capacidad de transporte de corriente también va a depender de la aplicación y del aislamiento.
En caso de duda, consulte al fabricante para mayor información.

Orientación de los paneles

La mayor parte de la energía que proviene del sol llega en línea recta. El módulo solar captará más energía si está "de cara" al sol, perpendicular a la línea recta entre la posición de la instalación y el sol. Obviamente, la posición del sol está cambiando constantemente con relación a la tierra, así

que necesitamos encontrar la posición óptima para nuestros paneles. La orientación de los mismos está determinada por dos ángulos, el **azimut, a** y la **inclinación** o **elevación, β.** El azimut es el ángulo que mide la desviación con respecto al sur en el hemisferio norte, y con respecto al norte, en el hemisferio sur. La inclinación es el ángulo formado por la superficie del módulo y el plano horizontal.

Azimut

El módulo debe orientarse hacia el ecuador terrestre (hacia el sur, en el hemisferio norte y hacia el norte en el hemisferio sur) de manera que durante el día el panel atrape la mayor cantidad de radiación ($a = 0^{o}$). ¡Es muy importante que ninguna parte del panel quede en la sombra! Examine los elementos que rodean el banco de paneles (árboles, edificios, paredes, otros paneles, etc.) para asegurarse de que no hagan sombra a sus paneles en ningún momento del día o del año. Es aceptable girar los paneles ± 20° hacia el este o hacia el oeste si se necesita ($a = \pm 20°$).

Inclinación

Una vez que se fija el azimut, el parámetro clave para nuestro cálculo es la inclinación del panel, que expresaremos como el ángulo beta (β). La altura máxima que el sol alcanza cada día va a variar, con un máximo en el día de solsticio de verano y un mínimo, el día del solsticio de invierno.

Idealmente, los paneles deberían rastrear esta variación, sin embargo, esto no siempre es posible por razones de costo. En instalaciones con equipos de telecomunicaciones es usual instalar el panel con una inclinación fija. En la mayor parte de los casos de telecomunicaciones, las demandas de energía del sistema son constantes a lo largo del año. Calcular la energía suficiente para el "peor mes" es una medida que nos servirá para el resto del año.

El valor de β debería maximizar la razón entre la oferta y la demanda de energía. Para instalaciones con un consumo consistente (o casi consistente) durante el año es preferible optimizar la instalación para que capture la radiación máxima durante los meses de "invierno".

Usted debería usar el valor absoluto de la latitud del lugar (ángulo F) con una adición de 10° ($\beta = | F | + 10°$).

Para instalaciones con menor consumo durante el invierno, el valor de la latitud del lugar puede ser usado como la inclinación del panel solar. De

esta manera, optimizamos el sistema para los meses de primavera y otoño ($\beta = |F|$).

Para instalaciones que se usen sólo en verano, se debería usar el valor absoluto de la altitud del lugar (ángulo F) con una disminución de 10° ($\beta = | F | - 10°$).

La inclinación del panel nunca debería ser menor de 15° para evitar la acumulación del polvo y la humedad sobre el mismo. En áreas donde hay nieve o hielo es importante proteger los paneles e inclinarlos a un ángulo de 65° o mayor. Si hay un incremento de consumo de energía considerable durante el verano, debería planificarse dos inclinaciones fijas: una posición para los meses de verano, y otra para los de invierno. Esto va a requerir de estructuras de soporte especiales y previsiones para cambiar la posición de los paneles.

Cómo dimensionar su sistema voltaico

Cuando escoja el equipo para satisfacer sus necesidades de energía, va a necesitar la determinación de, al mínimo, la siguiente información:

- El número y tipo de paneles solares que se necesitan para la captación de la energía solar necesaria para su carga.
- La capacidad mínima de la batería. La batería necesita almacenar energía suficiente para proveer energía durante la noche y en días de poco sol, y determinará el número de días de autonomía.
- Las características de los otros componentes (el regulador, cableado, etc.) necesarios para mantener la cantidad de energía generada y almacenada.

Los cálculos de dimensionado del sistema son importantes porque, a menos que los componentes del mismo estén balanceados, derrochamos energía (y al final, dinero). Por ejemplo, si instalamos más paneles de los necesarios para obtener más energía, las baterías deberían tener capacidad suficiente para almacenar esa cantidad extra producida.

Si el banco de baterías es muy pequeño y la carga no consume la energía a medida que se genera, la energía deberá desecharse. Un regulador con un amperaje menor del que se necesita, o un solo cable que sea demasiado pequeño pueden causar fallas (incluso incendio) y dejar la instalación

inservible.

Nunca olvide que la capacidad de un sistema fotovoltaico para producir y almacenar energía eléctrica es limitada.

Dejar un bombillo encendido accidentalmente durante el día puede gastar las reservas de energía antes de que llegue la noche, cuando ya no tenemos disponibilidad de energía adicional. La disponibilidad de “combustible” para un sistema fotovoltaico (es decir, radiación solar) puede ser difícil de predecir. De hecho, nunca es posible tener la seguridad de que un sistema autónomo va a proporcionar la energía necesaria en un momento determinado. Los sistemas solares están diseñados para un cierto consumo y si el usuario excede los límites planeados, fallará la provisión de energía.

El método de diseñado que proponemos consiste en calcular las necesidades de energía, y con base en esto, calcular un sistema que trabaje durante el mayor tiempo posible, de manera que sea lo más confiable posible. Por supuesto, si se instalan más paneles y más baterías, seremos capaces de captar y almacenar más energía con un incremento de la confiabilidad, pero también de costos.

En algunas instalaciones fotovoltaicas (como en el suministro de energía para equipos de telecomunicaciones en la dorsal (backbone) de una red, el factor de disponibilidad es más importante que el costo. En cambio para una instalación de cliente, el bajo costo es más importante. Encontrar el balance entre costo y disponibilidad no es tarea fácil, pero cualquiera sea su situación, debería ser capaz de determinar qué se espera de las opciones de su diseño y a qué precio.

El método que usaremos para dimensionar el sistema se conoce como el método del peor mes. Simplemente calculamos las dimensiones del sistema autónomo para que trabaje durante el mes en que las demandas de energía van a ser mayores con respecto a la energía solar disponible. Es el peor mes del año porque presentará la mayor relación entre energía solicitada y energía disponible. Al utilizar este método, la confiabilidad se considera estableciendo el máximo de días que el sistema puede trabajar sin recibir radiación solar (es decir, cuando el consumo se hace exclusivamente a expensas de la energía almacenada en la batería).

Esto se conoce como máximo de días de autonomía (N), es decir, el número de días nublados consecutivos en los que los paneles no colectan ninguna cantidad significativa de energía. Para determinar N, es necesario conocer la climatología del lugar, así como la relevancia económica y social de la

instalación. ¿Va a usarse para iluminar casas, un hospital, una fábrica, para un radio enlace, u otra aplicación? Recuerde que a medida que N es mayor, también aumenta la inversión en equipos y mantenimiento.
También es importante evaluar los costos logísticos de reemplazo de equipos.
No es lo mismo cambiar una batería descargada de una instalación en medio de la ciudad, que una en la cima de una torre de telecomunicaciones que se encuentra a horas, o días de camino a pie. Establecer el valor de N no es fácil porque hay muchos factores en juego y muchos no pueden ser evaluados con facilidad. Su experiencia va a jugar un importante papel en este punto del dimensionado. Un valor comúnmente usado para equipos críticos de telecomunicaciones es el de N = 5, mientras que para equipo cliente de bajo costo es posible reducir la autonomía a N = 3.

En el **Apéndice E: Energía solar: dimensionamiento** presentamos varias tablas que le facilitarán la recolección de los datos necesarios para el dimensionado del sistema. En el resto del capítulo explicaremos en detalle la información que necesita para recolectar datos o hacer estimados para el uso del método del "peor mes".

Qué datos recolectar

Latitud de la instalación. Recuerde usar un signo positivo en el hemisferio norte y uno positivo en el hemisferio sur.
Datos de radiación solar. Para el método del "peor mes" es suficiente conocer 12 valores: uno por cada mes. Los doce números son los valores promedio mensuales de la irradiación global diaria en plano horizontal, $G_{dm}(0)$, en kWh/m^2 por día. El valor mensual es la suma de los valores de irradiación global para cada día del mes, dividida por el número de días del mes.
Si usted tiene los datos en Joules (J), puede aplicar la siguiente conversión:

$1\ J = 2{,}78 \times 10^{-7}\ kWh$

Los datos de irradiación $G_{dm}(0)$ de muchos sitios del mundo están disponibles en tablas y bases de datos.
Usted debería buscar esta información en alguna estación meteorológica cercana a su sitio de implementación, pero no se sorprenda si no los encuentra en formato electrónico.
Es una buena idea consultar compañías que instalen sistemas fotovoltaicos

en el lugar ya que su experiencia puede ser muy valiosa.

No confunda “horas de sol” con el número de “horas de sol pico”. El número de horas de sol pico no tiene que ver con las horas sin nubosidad, sino se refiere a la cantidad de irradiación diaria. Un día de 5 horas de sol sin nubes, no necesariamente tiene esas horas cuando el sol está en su cenit.

Una hora de sol pico es un valor estandarizado de radiación solar de 1000 W/m^2 a 25°C. Así que cuando hablamos de 5 horas de sol pico (HSP), nos referimos a una radiación solar diaria de 5000 W/m^2 .

Características eléctricas de los componentes del sistema

Las características eléctricas de los componentes de su sistema debe proporcionarlas el fabricante. Es recomendable que usted realice sus propias medidas para controlar posibles desviaciones de las especificaciones nominales. Desafortunadamente, la desviación de los valores prometidos puede ser grande y no debe sorprenderle.

A continuación le presentamos los valores mínimos que debería tener presente antes de comenzar el dimensionado:

Paneles

Usted debería conocer el voltaje V_{Pmax} y la corriente I_{Pmax} en el punto de máxima potencia y en condiciones estándar.

Baterías

La capacidad nominal (para 100 horas de descarga) C_{NBat} , el voltaje operacional V_{NBat}, y, bien sea la profundidad máxima de descarga DoD_{max}, o la capacidad útil C_{UBat}.

También necesita conocer qué tipo de batería va a usar: plomo-ácido, gel, AGM, de tracción modificada, etc.
El tipo de batería es importante cuando haya que decidir los puntos de corte del regulador.

Regulador

Necesita saber el voltaje nominal V_{NReg}, y la coriente máxima a la que opera I_{maxReg}.

Convertidor/Inversor continua/alterna DC/AC

Si va a usar un convertidor, necesita saber el voltaje nominal V_{NConv}, la energía instantánea P_{IConv} y el rendimiento al 70% de la carga máxima H_{70}.

Equipo o carga

Es necesario saber el voltaje nominal V_{NC} y la potencia nominal de operación PC para cada equipo alimentado por el sistema. Para saber la energía total que nuestra instalación va a consumir es también importante tomar en cuenta el tiempo promedio que cada carga va a ser usada. ¿Es constante? ¿O va a usarse diariamente, semanalmente, mensualmente, anualmente? Considere cualquier cambio en el uso que pueda alterar la cantidad de energía que se necesitará (uso estacional, períodos escolares, etc.).

Otras variables

Aparte de las características eléctricas de los componentes de su carga es necesario considerar otros dos elementos antes de dimensionar el sistema: el número de días de autonomía y el voltaje de trabajo del sistema.

N: número de días de autonomía

Necesita decidir sobre el valor de N que establecerá un balance entre las condiciones meteorológicas, el tipo de instalación y el costo general. Es imposible asignarle un valor concreto a N válido para todo tipo de instalación, pero las tablas que se presentan a continuación le sugerirán algunos valores recomendados.

Tome estos valores como una aproximación y consulte con un experto en el área para tomar su decisión definitiva.

Luz solar disponible	Instalación Domestica	Instalación Crítica
Muy nublado	5	10
Variable	4	8
Soleado	3	6

V_N, voltaje nominal de la instalación

Los componentes de su sistema se escogen para operar a un voltaje nominal V_N , que es normalmente de 12 ó 24 voltios para sistemas pequeños. Si la potencia de consumo sobrepasa los 3 kW, el voltaje será de 48 V. La selección de V_N no es arbitraria, y depende de la disponibilidad del equipo.

Si el equipo lo permite, trate de fijar el voltaje nominal en 12 ó 24 V.

Muchas tarjetas de comunicación inalámbrica aceptan un rango amplio de voltaje de entrada y pueden ser usadas sin un convertidor. Si necesita alimentar diferentes equipos que trabajen a diferentes voltajes nominales, calcule el voltaje que minimice el consumo global incluyendo la energía de los convertidores de continua/continua y continua/alterna.

Procedimiento de cálculo

Hay tres pasos principales que se deben seguir para calcular la dimensión adecuada de su sistema:

1. **Calcule la energía solar disponible (la oferta).** Basándonos en estadísticas sobre radiación solar, la orientación y la inclinación óptima de los paneles, calculamos la energía solar disponible. Este estimado se hace en intervalos mensuales, reduciendo los datos a 12 valores. Este estimado es un buen compromiso entre precisión y simplicidad.

2. **Estime la energía eléctrica que necesita (la demanda)**. Tome nota del consumo de energía característico del equipo escogido así como del uso estimado. Luego calcule la energía eléctrica que necesita mensualmente. Debería tomar en cuenta las fluctuaciones de uso debido a variaciones entre invierno y verano; períodos de lluvia/sequía; período de clases/vacaciones, etc. El resultado deben ser 12 valores de demanda de energía, una para cada mes del año.

3. **Calcule la dimensión ideal del sistema (el resultado)**.
   Con los datos procedentes del "peor mes", cuando la relación entre la energía solar necesaria, y la energía disponible es la más grande, calculamos:

   - La corriente que el banco de paneles necesita proporcionar, lo que determinará la cantidad mínima de paneles necesitados.

   - La capacidad de almacenamiento de energía necesaria para cubrir el número mínimo de días de autonomía, lo que va

a determinar el número de baterías requerido.

- Las características eléctricas del regulador.
- La longitud y las secciones necesarias de cables para la conexión eléctrica.

Corriente necesaria en el peor mes

Para cada mes se necesita calcular el valor I_m que es la corriente máxima diaria que un banco de paneles operando al voltaje nominal V_N necesita proporcionar, en un día con una irradiación G_{dm} por mes "m", y paneles de una inclinación de β grados.
El I_m (PEOR MES) va a ser el valor más grande de I_m, y el dimensionado del sistema se basa en los datos de este mes.
Los cálculos de G_{dm}(ß) para un cierto sitio pueden hacerse con base en G_{dm}(0), usando un programa de computación tipo PVSYST (http://www.pvsyst.com/), o PVSOL (http://www.solardesign.co.uk/).
Debido a pérdidas en el regulador y las baterías, y debido al hecho de que los paneles no siempre trabajan en su punto de máxima potencia, la corriente requerida I_{mMAX} se calcula así:

$$I_{mMAX} = 1.21\ I_m\ (PEOR\ MES)$$

Una vez que se haya determinado el peor mes, el valor de I_{mMAX}, y la cantidad total de energía que necesite, E_{TOTAL} (PEOR MES), puede proceder al cálculo final. E_{TOTAL} es la suma de todas las cargas de corriente continua (DC) y alterna (AC), en vatios. Para calcular E_{TOTAL}, vea el **Apéndice E: Energía Solar: Dimensionamiento.**

Número de Paneles

Combinando los paneles solares en serie y en paralelo podemos obtener la corriente y el voltaje deseados. Cuando los paneles están conectados en serie, el voltaje total es igual a la suma de los voltajes individuales de cada módulo, mientras que la corriente permanece inalterada. Cuando se conectan los paneles en paralelo, las corrientes se suman, mientras que el voltaje permanece inalterado. Es muy importante usar paneles que tengan aproximadamente las mismas características cuando construya su banco. Debería tratar de conseguir paneles con V_{Pmax} un poco mayor que el voltaje

nominal del sistema (12, 24 ó 48 V).
Recuerde que debe proporcionar una cantidad un poco mayor que el voltaje nominal de la batería para poder cargarla. Si no le es posible encontrar un panel único que satisfaga sus necesidades, va a necesitar conectar varios paneles en serie para obtener el voltaje deseado. El número de paneles en serie N_{ps} es igual al voltaje nominal del sistema dividido por el voltaje de un solo panel, con aproximación al entero superior.

$$N_{ps} = V_N / V_{Pmax}$$

Para calcular el número de paneles en paralelo (N_{pp}), necesitas dividir el I_{mMAX} por la corriente de un solo panel en el punto de máxima potencia I_{pmax}, con aproximación al entero superior.

$$N_{pp} = I_{mMAX} / I_{Pmax}$$

El número total de paneles es el resultado de multiplicar el número de paneles en serie (para fijar el voltaje) por el número de paneles en paralelo (para fijar la corriente).

$$N_{TOTAL} = N_{ps} * N_{pp}$$

Capacidad de la batería o acumulador

La batería determina el voltaje global del sistema y necesita tener la capacidad suficiente para proporcionar energía a la carga cuando no haya suficiente radiación solar. Para estimar la capacidad de nuestra batería, calculamos primero la capacidad de energía requerida por nuestro sistema (capacidad necesaria, CNEC). La capacidad necesaria depende de la energía disponible durante el "peor mes" y del número de días de autonomía deseados (N).

$$C_{NEC}\ (Ah) = E_{TOTAL}(PEOR\ MES)(Wh) / V_N(V) * N$$

La capacidad nominal de la batería C_{NOM} necesita ser mayor que la C_{NEC} ya que no podemos descargar totalmente una batería. Para calcular el tamaño de la batería necesitamos considerar la profundidad máxima de descarga (DoD) que permite la batería.

$$C_{NOM}(Ah) = C_{NEC}(Ah) / DoD_{MAX}$$

Para calcular el número de baterías en serie (N_{bs}), dividimos el voltaje nominal de nuestra instalación (V_N) por el voltaje nominal de una batería sola (V_{NBat}):

$$N_{bs} = V_N / V_{NBat}$$

Regulador

Una precaución importante es usar siempre reguladores en serie, nunca en paralelo. Si su regulador no suministra la corriente requerida por el sistema, necesita comprar otro regulador con una corriente de trabajo más grande. Por razones de seguridad, un regulador debe ser capaz de operar con una corriente I_{maxReg} por lo menos 20% más grande que la intensidad máxima proporcionada por el banco de paneles:

$$I_{maxReg} = 1.2\ N_{pp}\ I_{PMax}$$

Inversor continua/alterna DC/AC

La energía total que se necesita para el equipo de alterna (AC) se calcula incluyendo todas las pérdidas ocasionadas por el inversor o convertidor de continua/alterna (DC/AC) Cuando escoja un inversor, recuerde que su rendimiento varía de acuerdo con la cantidad de energía demandada. Un inversor tiene un mayor rendimiento cuando trabaja con valores cercanos a los especificados. Usar un inversor de 1.500 vatios para alimentar una carga de 25 vatios es altamente ineficiente. Para evitar este gasto de energía se deben considerar no las potencias pico de todo el equipo, sino las potencias pico de las partes del equipo que vayan a trabajar simultáneamente.

Cables

Una vez que conozca el número de paneles y baterías, el tipo de reguladores e inversores que quiere usar, debe calcular la longitud y espesor de los cables que se necesitan para conectar todos los componentes juntos.

El **largo** va a depender del sitio de su instalación. Debería tratar de minimizar el largo de los cables entre el regulador, los paneles y las baterías. Usar cables cortos va a minimizar la pérdida de energía y el gasto en cableado.

El **espesor** se escoge en relación con el largo del cable y la corriente máxima que debe transportar.

El objetivo es minimizar las caídas de voltaje. Para calcular el espesor S de

un cable es necesario saber:

- la corriente máxima I_{MC} que va a circular por el cable. En el caso del subsistema del panel-baterías, es I_{mMAX} calculada por cada mes. En el subsistema baterías-cargas, va a depender de la manera en que las baterías estén conectadas;
- la caída del voltaje (V_a-V_b) que consideramos aceptable en el cable. La caída del voltaje que resulta de la suma de las caídas individuales posibles se expresa como un porcentaje del voltaje nominal de la instalación.

Ejemplo de algunos valores máximos típicos:

Componente	Caída del Voltaje (% de V_N)
Banco de Paneles -> Batería	1.00%
Batería -> Convertidor	1.00%
Línea Principal	3.00%
Línea Principal (Iluminación)	3.00%
Línea Principal (Equipo)	5.00%

Caídas de voltaje aceptable más comunes

La sección del cable se determina por la ley de Ohm:

$$S(mm^2) = r(\Omega mm^2/m)L(m)\ I_{mMAX}(A)/\ (V_a\text{-}V_b)(V)$$

donde *S* es la sección, r es resistividad (propiedad inherente del material: para el cobre es de 0,01286 Ωmm^2/ m), y L es el largo. Vamos a escoger *S* de acuerdo con la disponibilidad de cables en el mercado.
Se debería escoger la sección inmediatamente superior a la que se obtiene por la fórmula.
Por razones de seguridad, hay valores mínimos para el cable que conecta los paneles con la batería. Este valor es de 4 mm^2.

Costo de una instalación solar

Aunque la energía solar en sí misma es gratis, el equipo que se necesita para su aprovechamiento no lo es.
Usted va a necesitar no sólo comprar equipo para transformar la energía solar en electricidad y almacenarla para su uso, sino que también debe gastar en mantenimiento y reemplazo de los varios componentes del sistema.
El problema del reemplazo de equipo es a menudo pasado por alto, y un sistema de energía solar no se puede implementar sin un plan adecuado de mantenimiento. Para calcular el costo real de su instalación vamos a proporcionarle un ejemplo ilustrativo.
Lo primero que hay que hacer es calcular el costo de la inversión inicial.

Descripción	Número	Costo Unitario	Subtotal
Panel Solar de 60W (unos $4/W)	4	$300	$1.200
Regulador de 30A	1	$100	$100
Cable (metros)	25	$1 /metro	$25z
Batería de Ciclo Profundo de 50 Ah	6	$150	$900
		Total	$2.225

El cálculo de nuestro costo de inversión se hace relativamente fácil una vez que el sistema ha sido dimensionado. Sólo se necesita ahora añadir el precio por cada pieza del equipo, y el costo de mano de obra de instalación y cableado de todo el equipo.
Por razones de simplicidad no se incluye aquí los costos de transporte e instalación, pero no deberían dejarse de lado.
Para calcular cuánto cuesta en realidad operar un sistema debemos calcular la duración de cada pieza y la frecuencia de reemplazo. En el léxico de contaduría esto se llama ***amortización***. Nuestra nueva tabla, entonces, sería algo así:

Descripción	Número	Costo Unitario	Subtotal	Vida útil (años)	Costo anual
Panel Solar de	4	$300	$1.200	20	$60

60W					
Regulador de 30A	1	$100	$100	5	$20
Cable (metros)	25	$1/ metro	$25	10	$2,50
Batería de Ciclo Profundo de 50 Ah	6	$150	$900	5	$180
		Total	$2.225	Costo Anual	$262,50

Como puede observar, una vez que se ha hecho la primera inversión, se espera un costo anual de $262,50. El costo anual es el estimado del capital anual necesario para reemplazar los componentes del sistema una vez que estos agotan su vida útil.

MANTENIMIENTO, MONITOREO Y SOSTENIBILIDAD

15. MANTENIMIENTO Y SOLUCIONES

Introducción

La manera de establecer la infraestructura de soporte de su red es tan importante como el tipo de equipamiento que utilice. A diferencia de las conexiones cableadas, los problemas con las redes inalámbricas a menudo son invisibles, y pueden requerir más capacidades y más tiempo para diagnosticarlos y remediarlos. La interferencia, el viento y otras obstrucciones físicas pueden causar fallas en una red que llevaba tiempo funcionamiento satisfactoriamente. Este capítulo detalla una serie de estrategias para ayudarlo/la a formar un equipo de gente que pueda dar soporte a su red de forma efectiva. También describiremos algunas técnicas estándares de resolución de problemas que ayudan efectivamente a solucionar problemas de redes en general.

Conformar el equipo

Cada pueblo, compañía o familia, tiene algunas personas que están intrigadas por la tecnología. Son aquellas a quienes encontramos empalmando el cable de televisión, reparando un televisor o soldando una nueva pieza a una bicicleta. Este tipo de gente se va a interesar por su red y querrá aprender tanto como le sea posible. Aunque estas personas son recursos muy valiosos, debe evitar impartir todo el conocimiento especializado sobre las redes inalámbricas a una sola persona, porque si su único especialista pierde interés o encuentra un trabajo mejor remunerado en otro lugar, se va a llevar el conocimiento consigo cuando se vaya.

También puede haber muchos adolescentes jóvenes y ambiciosos o adultos jóvenes que se interesan por el tema y tienen tiempo para escuchar, ayudar y aprender acerca de la red.

Ellos son de gran ayuda y van a aprender rápidamente, pero el equipo debe enfocar su atención en aquellos/as que sean los mejores para dar soporte a la red en los meses y años siguientes.

Lo más probable es que los adultos jóvenes y los adolescentes se marchen a la universidad o a encontrar empleo, especialmente los ambiciosos, que son a los/las que les gustaría involucrarse.

Estos jóvenes también tienen poca influencia en la comunidad, donde una persona mayor es probable que tenga más capacidad para tomar decisiones que afecten a la red positivamente. A pesar de que estas personas puedan tener menos tiempo para aprender y parezcan menos interesados/as, su contribución y educación adecuada acerca del sistema puede ser significativa.

Por lo tanto, una estrategia clave para armar un equipo de soporte es balancear y distribuir el conocimiento entre aquellos que son los/las más capacitados para darle soporte a la red a largo plazo. Si bien debe involucrar a los/las jóvenes, no les debe dejar capitalizar el uso o el conocimiento de estos sistemas. Encuentre gente que esté comprometida con la comunidad, que tenga sus raíces en ella, que puedan ser motivados, y enséñeles. Una estrategia complementaria es repartir funciones y obligaciones y documentar toda la metodología y procedimientos.

De esta forma la gente puede ser entrenada fácilmente y sustituida con poco esfuerzo.

Por ejemplo, en un determinado proyecto, el equipo de entrenamiento seleccionó a un brillante joven recién graduado de la universidad que había vuelto a su pueblo; él estaba muy motivado y aprendió rápidamente. Como aprendió tan rápido, se le enseñó más de lo que se había previsto, y era capaz de lidiar con una variedad de problemas, desde arreglar una computadora a rearmar el cable Ethernet. Desafortunadamente, dos meses después de emprender el proyecto le llegó una oferta para un trabajo en el gobierno y dejó la comunidad. Ni siquiera con la oferta de un salario similar se le pudo retener, ya que la perspectiva de un trabajo estable en el gobierno era más atractiva. Todo el conocimiento de la red y cómo realizar su soporte se fue con él. El equipo de entrenamiento tuvo que volver y comenzar el entrenamiento otra vez. La siguiente estrategia fue dividir funciones y entrenar gente que estuviera establecida de forma permanente en la comunidad: gente que tuviera hijos y casas, y que ya tuviera trabajo. Llevó el triple de tiempo enseñarles a tres personas hasta que alcanzaron el nivel de entrenamiento del joven universitario, pero la comunidad retuvo ese conocimiento por mucho más tiempo.

Con esto queremos sugerirle que seleccionar por usted mismo a quien se va a involucrar en el proyecto, a menudo no es el mejor enfoque. En general, es mejor encontrar una organización local o un/a administrador/a local, y trabajar con ellos/as para encontrar el equipo técnico adecuado.

Los valores, la historia, las políticas locales y muchos otros factores pueden ser importantes para ellos/as, mientras que pueden ser completamente incomprensibles para gente que no es de esa comunidad. El mejor enfoque es entrenar a su socio local para darle cierto criterio (asegurándose de que lo comprenden) y para marcar límites firmes.

Dichos límites deben incluir reglas acerca del favoritismo y clientelismo, aunque éstas deben considerar la situación local. Probablemente sea imposible decirles que usted no puede contratar familiares, pero deben existir inspecciones y balances. Si tenemos un/a candidato/a que sea un familiar, debe haber un criterio claro, y una segunda autoridad que decida sobre su candidatura. También es importante que el socio local tenga esa autoridad y que no sea influido por los organizadores del proyecto, porque de otro modo se compromete su habilidad gerencial. Los socios locales deben ser capaces de determinar quién va a ser la mejor persona para trabajar con ellos. Si son bien instruidos sobre este proceso, entonces los requerimientos de personal serán cumplidos a cabalidad.

La resolución de problemas y el soporte técnico son como el arte abstracto. La primera vez que usted ve una pintura abstracta puede que le parezca un conjunto de pinceladas al azar. Luego de reflexionar en la composición durante un tiempo, puede que comience a apreciar la obra como un conjunto, y la coherencia "invisible" se vuelva real. La mirada de un neófito a una red inalámbrica puede identificar antenas, cables y computadoras, pero le puede tomar bastante tiempo apreciar el objetivo de la red "invisible". En áreas rurales, es posible que la gente de la localidad deba hacer una inmensa evolución en su comprensión antes de que pueda apreciar una red invisible que fue instalada en su pueblo. Por lo tanto se necesita una introducción paulatina que les haga más fácil aceptar y apropiarse de la tecnología. El mejor método es fomentar el compromiso de la comunidad. Una vez que los/las participantes hayan sido seleccionados y se hayan comprometido con el proyecto, involúcrelos/as tanto como sea posible. Déjelos/as "manejar". Entrégueles la pinza crimpeadora (*crimper*), o el teclado y muéstreles cómo hacer el trabajo. Aunque usted no tenga tiempo para explicar cada detalle, y a sabiendas de que haciéndolo de esta manera va a tomar mucho más tiempo, ellos/as necesitan involucrarse físicamente y ver no sólo lo que ha sido hecho, sino también cuánto trabajo se ha hecho.

El método científico se enseña prácticamente en todas las escuelas occidentales.

Mucha gente lo aprende durante sus clases de ciencia en la secundaria. Para decirlo simplemente, se toma un conjunto de variables, luego se eliminan lentamente dichas variables a través de pruebas binarias hasta quedarse con una, o pocas posibilidades. Con esas posibilidades en mente, se completa el experimento. Luego se prueba si el experimento produce algo similar al resultado esperado, de lo contrario se calcula nuevamente el resultado esperado y se intenta de nuevo. Al campesino típico se le pudo haber explicado este concepto, pero probablemente no haya tenido la oportunidad de aplicarlo para resolver problemas complejos. Aunque estén familiarizados con el método científico, es probable que no hayan pensado en aplicarlo para resolver problemas reales.

Este método es muy efectivo a pesar de que puede llegar a consumir mucho tiempo. Se puede acelerar haciendo suposiciones lógicas. Por ejemplo, si un punto de acceso que venía funcionando hace mucho, deja de hacerlo repentinamente luego de una tormenta, se puede sospechar que hay un problema con el abastecimiento eléctrico y por lo tanto obviar la mayor parte del procedimiento.

Las personas que han sido adiestradas para dar soporte deben aprender como resolver los problemas utilizando este método, ya que va a haber momentos en los que el problema no es ni conocido ni evidente. Se pueden crear simples árboles de decisión, o diagramas de flujo, e intentar eliminar las variables para aislar el problema. Por supuesto, esos cuadros no deben ser seguidos ciegamente.

A menudo es más sencillo enseñar este método utilizando primero un problema no tecnológico. Digamos, haga que su estudiante desarrolle un procedimiento de resolución para un problema sencillo y familiar, como por ejemplo, un televisor a batería. Para empezar, sabotee el aparato: póngale una batería sin carga, desconecte la antena e inserte un fusible roto. Pruebe al estudiante, dejándole en claro que cada problema muestra síntomas específicos, e indíquele la manera de proceder.

Una vez que haya reparado el televisor, hágalo aplicar este procedimiento a un problema más complicado. En una red, usted puede cambiar una dirección IP, cambiar o dañar cables, utilizar el ESSID equivocado u orientar la antena en la dirección equivocada. Es importante que los/las aprendices desarrollen una metodología y un procedimiento para resolver estos problemas.

Técnicas adecuadas para detectar problemas

Ninguna metodología de detección de problemas puede cubrir por completo todos aquellos con los que usted se va a encontrar cuando trabaja con redes inalámbricas, pero a menudo los problemas caen dentro de uno de los pocos errores comunes. A continuación se presentan algunos puntos que se deben recordar, y que pueden hacer que su esfuerzo para resolver el problema vaya en la dirección correcta.

- **No entre en pánico.** Si usted está arreglando un sistema, significa, con seguridad, que el mismo estaba funcionando muy recientemente. Antes de sobresaltarse y hacer cambios impulsivamente, analice la escena y determine exactamente lo que está roto. Si tiene un registro histórico, o estadísticas de funcionamiento, mucho mejor. Asegúrese de recolectar la información en primer lugar para poder tomar una decisión bien informada antes de hacer cambios.

- **Haga una copia de seguridad.** Esto se debe hacer antes de que usted detecte problemas y le servirá después. Si va a hacer una actualización compleja de software al sistema, tener una copia de seguridad significa que puede restaurarlo rápidamente a la configuración previa y comenzar de nuevo. Cuando resolvemos problemas muy complejos, tener una configuración que "más o menos funciona" puede ser mucho mejor que tener una que no funciona para nada (y que no puede restaurar fácilmente desde la memoria).

- **¿Está conectado?** Este paso a menudo se pasa por alto hasta que se exploran muchas otras posibilidades. Los enchufes pueden desconectarse muy fácilmente, ya sea accidental o intencionalmente. ¿El cable está conectado a una buena fuente de energía? ¿El otro extremo está conectado a su equipo? ¿La luz de energía está encendida? Esto puede sonar algo tonto, pero usted se verá aún más tonto si pierde mucho tiempo en probar la línea de alimentación de la antena sólo para comprobar que el AP estuvo desenchufado todo ese tiempo. Confíe en nosotros, esto sucede más a menudo de lo que la mayoría queremos admitir.

- **¿Cuál fue la última cosa que cambiamos?** Si usted es la única persona con acceso a sistema, ¿cuál fue el último cambio que hizo? Si otros tienen acceso a él, ¿cuál fue el último cambio que hicieron y cuándo? ¿Cuándo fue el último momento en el que el sistema funcionó? A menudo los cambios tienen consecuencias imprevistas que pueden no ser notadas inmediatamente. Deshaga ese cambio, y vea el efecto que tiene en el problema.

- **Mire los sellos de fecha/hora de los archivos.** Todo archivo en un computador moderno tiene un sello de fecha-hora asociado con él, que indica cuándo fue creado o modificado por última vez. En un sistema que funciona adecuadamente estos sellos se van a mantener durante meses, o años. Si el sistema o red estaba funcionando bien hasta hace más o menos una hora, los archivos que tienen el sello de hace unos minutos hasta una hora podrían darnos una pista de qué ha cambiado en ese lapso.

- **El bueno conocido.** Esta idea se aplica tanto al equipamiento como a los programas. Un ***bueno conocido*** es cualquier componente que se pueda reemplazar en un sistema complejo para verificar que sus contrapartes estén en buenas condiciones de funcionamiento. Por ejemplo, puede llevar junto con sus herramientas, un cable Ethernet previamente probado. Si sospecha que hay problemas con el cable que está en la instalación, sencillamente puede intercambiar el cable sospechoso con el bueno conocido y ver si las cosas mejoran. Esto es mucho más rápido y menos propenso a los errores que rearmar un cable, y le dice inmediatamente si el cambio solucionó el problema. De igual manera, usted puede tener una batería de repuesto, un cable de antena, o un CD-ROM con una buena configuración conocida para el sistema. Cuando solucionamos problemas complicados, guardar su trabajo en un punto dado nos permite retornar a un estado bueno conocido, aún si el problema no se ha solucionado por completo.

- **Determine lo que todavía está funcionando.** Esto le va a ayudar a "cercar el problema". Como los sistemas complejos como una red inalámbrica están conformados por muchos componentes, es probable que el problema esté afectando sólo a algunos de ellos. Si, por ejemplo, alguien en un laboratorio se queja de que no tiene

acceso a Internet, chequee si otras personas en este espacio tienen el mismo problema. ¿Hay conectividad en otros laboratorios o espacios del edificio? Si el problema se restringe a un sólo usuario o en un sólo salón, debe concentrar sus esfuerzos en los equipos de ese espacio. Si el apagón es más extenso, tal vez examinar los equipos desde donde llega su conexión externa sea más apropiado.

- **No lo dañe.** Si no comprende en su totalidad cómo funciona un sistema, no dude en llamar a un experto. Si no está seguro de si un cambio en particular va a dañar otras partes del sistema, entonces encuentre a alguien con más experiencia, o busque una forma de probar su cambio sin hacer daño. Poner una moneda en lugar de un fusible puede resolver el problema inmediato, pero también puede incendiar el edificio.

Es poco probable que la gente que diseñó su red esté disponible veinticuatro horas al día para resolver los problemas cuando aparecen. Aunque su equipo de soporte sea muy capaz de resolver problemas, puede que no sea lo suficientemente competente como para configurar un enrutador desde cero, o ponerle el conector a un cable LMR-400. A menudo es mucho más eficiente tener varios componentes de respaldo a mano, y entrenar a su equipo para reemplazar por completo la pieza rota. Esto puede significar tener un punto de acceso, o un enrutador preconfigurado, guardados en un gabinete cerrado, claramente etiquetado y almacenado junto con los cables de respaldo y las fuentes de alimentación. Su equipo puede cambiar el elemento que funciona mal y enviarlo a un experto para que lo repare o coordinar para que se envíe otro equipo de respaldo. Mantener los respaldos seguros y reemplazarlos cuando los usamos puede ahorrarnos mucho tiempo a todos.

Problemas comunes de las redes

A menudo los problemas de conectividad provienen de la rotura de componentes, un clima adverso o simplemente un problema de configuración. Una vez que su red esté conectada a Internet o abierta al público en general, van a aparecer una gran cantidad de amenazas provenientes de los mismos usuarios. Esas amenazas pueden estar en un rango desde las benignas, hasta las indiscutiblemente malévolas, pero todas van a tener impacto en su red si no está configurada correctamente.

Esta sección se enfoca en algunos problemas comunes encontrados una vez que su red es utilizada por seres humanos reales.

Sitios web alojados localmente

Si una universidad aloja su sitio web localmente, los visitantes del sitio desde fuera del campus y del resto del mundo van a competir con los trabajadores de la universidad por el ancho de banda. Esto incluye el acceso automatizado desde los motores de búsqueda que periódicamente 'escanean' su sitio por completo. Una solución para este problema es utilizar un DNS dividido y un servidor espejo. La universidad establece una copia de sus sitios web en un servidor que puede ser una compañía de almacenamiento web (*hosting*) europea, y utiliza el DNS dividido para direccionar a todos los usuarios de fuera de la universidad hacia el sitio espejo, mientras que los usuarios de la universidad acceden al mismo sitio pero a nivel local.

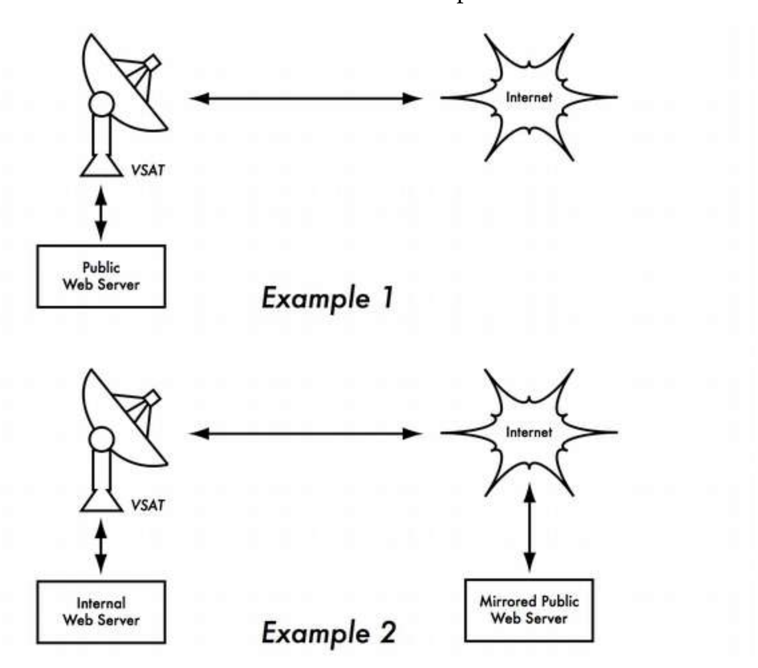


Figura MS 1: En el ejemplo 1, todo el tráfico del sitio web que viene desde Internet debe atravesar el VSAT. En el ejemplo 2, el sitio web público es alojado en un servicio europeo rápido, mientras que en el servidor interno se mantiene una copia para tener un acceso local muy rápido. Esto mejora la conexión del VSAT y reduce los tiempos de carga para los usuarios del sitio web

Proxys abiertos

Un servidor proxy debe configurarse para aceptar solamente conexiones desde la red de la universidad, no desde el resto de Internet. Esto se debe a que gente de todos lados va a conectarse y utilizar los proxys abiertos por una variedad de razones, como por ejemplo evitar pagar por ancho de banda internacional. La forma de configurarlo depende del servidor proxy que usted use. Por ejemplo, puede especificar el rango de direcciones IP para la red del campus en su archivo **squid.conf** de manera que esta sea la única red que puede utilizar Squid. Alternativamente, si su servidor proxy está detrás de un cortafuego, puede configurar el cortafuego para que le permita solamente a los servidores internos que se conecten al puerto proxy.

Servidores de retransmisión abiertos

Un servidor de correo electrónico configurado incorrectamente puede ser encontrado por gente inescrupulosa, y usado como un servidor de retransmisión para enviar grandes cantidades de mensajes y de correo no deseado (*spam*).
Ellos lo hacen para ocultar la verdadera fuente del correo no deseado y para evitar ser atrapados. Para detectar esta vulnerabilidad, haga la siguiente prueba en su servidor de correo electrónico (o en el servidor SMTP que actúa como servidor de retransmisión en el perímetro de la red del campus). Use ***telnet*** para abrir una conexión al puerto 25 del servidor en cuestión.

telnet mail.uzz.ac.zz 25

Si se permite conversación de línea de comando interactiva (como el ejemplo que sigue), el servidor está abierto para retransmitir:

MAIL FROM: spammer@waste.com
250 OK - mail from
RCPT TO: innocent@university.ac.zz
250 OK - rcpt to spammer@waste.com

En su lugar, la respuesta después del primer **MAIL FROM** debe ser algo así:

550 Relaying is prohibited.

Una prueba en línea como ésta, así como información acerca de este problema, están disponibles en sitios como:

http://www.mailradar.com/openrelay/ or http://www.checkor.com/

Como aquellos que envían correos masivos tienen métodos automatizados para encontrar los servidores de retransmisión abiertos, una institución que no proteja sus sistemas de correo es casi seguro que va a ser víctima de abusos.

Configurar el servidor de correo para que no sea un relevador abierto consiste en especificar las redes y *hosts* que están autorizados para transmitir mensajes a través de él en el MTA (por ejemplo, Sendmail, Postfix, Exim, o Exchange). Este probablemente va a ser el rango de direcciones IP de la red del campus.

Conexiones *peer-to-peer* (P2P)

El abuso del ancho de banda a través de programas para compartir archivos entre pares (*P2P*) se puede prevenir de las siguientes formas:

No permita la instalación de nuevos programas en las computadoras del campus. Si no damos acceso administrativo a los usuarios regulares hacia las PC de estaciones de trabajo es posible prevenir la instalación de aplicaciones devoradoras de ancho de banda.

Muchas instituciones también estandarizan la configuración de sus máquinas, instalando el sistema operativo requerido en una computadora, luego instalan todas las aplicaciones y las configuran de una forma óptima, incluyendo la imposibilidad de que los usuarios instalen nuevas aplicaciones. Una imagen del disco de esta PC se clona a todas las otras PC utilizando un programa como Partition Image (http://www.partimage.org/) o también Drive Image Pro (http://www.powerquest.com/).

Es probable que de vez en cuando los usuarios puedan eludir el control y consigan instalar nuevo software o dañar el que ya tenía instalado la computadora (provocando por ejemplo que esta se "cuelgue" a menudo). Cuando esto pasa, un administrador simplemente puede restablecer la imagen del disco, logrando que el sistema operativo y todo el software en la computadora sean exactamente como se especificó originalmente.

Programas que se instalan a sí mismos (desde Internet)

Existen programas que se instalan a sí mismos y luego utilizan ancho de banda –por ejemplo el denominado Bonzi-Buddy, el Microsoft Network, y otros tipos de "gusanos". Algunos programas son espías, y permanecen enviando información sobre los hábitos de búsqueda (y de consumo) de un usuario hacia una compañía en algún lugar de Internet. Estos programas se previenen, hasta cierto punto, educando a los usuarios y cerrando las PC para evitar el acceso como administrador a los usuarios normales. En otros casos, tenemos soluciones de software para encontrar y remover estos programas problemáticos, como Spychecker (*http://www.spychecker.com/*) y Ad-Aware (*http://www.lavasoft.de/*).

Actualizaciones de Windows

Los últimos sistemas operativos de Microsoft Windows suponen que una computadora con una conexión LAN tiene un buen enlace a Internet, y descarga automáticamente parches de seguridad, correctores de fallas y mejoradores, desde el sitio web de Microsoft. Esto puede consumir grandes cantidades de ancho de banda en un enlace a Internet costoso. Los dos posibles enfoques para este problema son:

- **Deshabilitar las actualizaciones de Windows en todas las estaciones de trabajo**. Las actualizaciones de seguridad son muy importantes para los servidores, pero es algo discutible que las necesiten las estaciones de trabajo de una red privada protegida, como la red de un campus.

- **Instalar un Servidor de Actualización de Software.** Este es un programa gratuito de Microsoft que le permite descargar todas las actualizaciones de Microsoft durante la noche al servidor local y luego distribuirlas desde allí a las estaciones de trabajo cliente.
  De esta forma las actualizaciones de Windows utilizarán el ancho de banda del enlace a Internet durante el día. Desafortunadamente, para que esto funcione, todos los PC cliente deben configurarse para utilizar el Servidor de Actualización de Software.
  Si usted tiene un servidor DNS flexible, también puede configurarlo para que responda todas las solicitudes al sitio web windowsupdate.microsoft.com, y lo redireccione hacia su servidor de actualización. Esta es una buena opción sólo para redes muy grandes, pero puede ahorrar una incalculable cantidad de ancho de banda de Internet.

Programas que suponen un enlace de gran ancho de banda

Además de las actualizaciones de Windows, muchos programas y servicios presuponen que el ancho de banda no es un problema, y por lo tanto consumen ancho de banda por motivos imposibles de predecir por el usuario. Por ejemplo, los paquetes anti-virus (como Norton AntiVirus) se auto-actualizan automáticamente y directamente desde Internet. Es mejor si estas actualizaciones se distribuyen desde un servidor local.

Otros programas como el RealNetworks para reproducir videos, descargan automáticamente actualizaciones y anuncios, e igualmente registran los patrones de uso y los envían de vuelta a un sitio en Internet. *Applets* aparentemente inofensivas (como Konfabulator y Dashboard widgets) hacen un sondeo continuo de los usuarios de Internet que puede ser de bajo consumo de ancho de banda (como informe del tiempo o noticias actuales), o de gran consumo de ancho de banda (como webcams). Estas aplicaciones deben limitarse o bloquearse totalmente. Las últimas versiones de de Windows y Mac OS X tienen un servicio de sincronización de tiempo. Esto mantiene la precisión del reloj del computador conectándolo a servidores de tiempo en Internet. Es más eficiente instalar un servidor local de tiempo y distribuir el tiempo preciso desde allí en lugar de ocupar el enlace a Internet con estas peticiones.

Gusanos y virus

Los gusanos y los virus pueden generar una gran cantidad de tráfico. Por ejemplo el gusano W32/Opaserv aún prevalece, a pesar de que es muy viejo. Se esparce a través de los recursos compartidos de Windows y es detectado por otras personas en Internet porque intenta esparcirse aún más. Por esta razón es esencial que haya una protección antivirus instalada en todas las PC. Más esencial aún es la educación de los usuarios en cuanto a no ejecutar archivos adjuntos, así como a no dar respuesta a correos no deseados. De hecho, debería haber una política de que ni las estaciones de trabajo, ni el servidor, puedan ejecutar servicios que no estén utilizándose. Una computadora no debería tener recursos compartidos, a menos que fuera un servidor de archivos; y un servidor no debería ejecutar servicios innecesarios. Por ejemplo, los servidores Windows y Unix generalmente activan un servicio de servidor web por defecto. Éste debería deshabilitarse si dicho servidor tiene una función diferente; cuantos menos servicios se puedan ejecutar en una computadora, menos posibilidades tiene de ser atacada.

Círculo vicioso de reenvío (*forward*) de correos electrónicos

Ocasionalmente, un error cometido por un único usuario puede llegar a causar un problema serio. Por ejemplo, un usuario cuya cuenta universitaria está configurada para reenviar todo el correo a su cuenta personal en Yahoo. El usuario se va de vacaciones, y todos los correos que le fueron enviados se siguen reenviando a su cuenta en Yahoo, la cual puede crecer sólo hasta 2 MB. Cuando la cuenta de Yahoo se llene, va a comenzar a rebotar los correos hacia la cuenta de la universidad, que inmediatamente los va a reenviar a la cuenta de Yahoo. Un círculo vicioso de correo electrónico se forma cuando se envían y reenvían cientos de miles de correos, generando un tráfico masivo y congestionando los servidores de correo.

Existen opciones dentro de los servidores de correo que son capaces de reconocer estos círculos. Estas opciones deben activarse por defecto. Los administradores también deben tener cuidado de no apagarlas por error. Debe también evitarse instalar un sistema de reenvío SMTP que modifica los encabezados de los correos de tal forma que el servidor de correo no pueda reconocer el círculo vicioso que se ha formado.

Descargas pesadas

Un usuario puede iniciar varias descargas simultáneas, o descargar grandes archivos, como por ejemplo, 650 MB de imágenes ISO, acaparando la mayor parte del ancho de banda. La solución a este tipo de problemas está en el entrenamiento, hacer descargas diferidas, y monitoreo.

La descarga diferida se puede implementar al menos de dos formas:

- En la Universidad de Moratuwa, se implementó un sistema de URL redireccionado. A los usuarios que acceden a direcciones **ftp://** se les ofrece un directorio donde cada archivo listado tiene dos enlaces: uno para la descarga normal, y otro para la descarga diferida. Si se selecciona la descarga diferida, el archivo especificado se pone en cola para descargarlo más tarde, y al usuario se le notifica por correo electrónico cuando la descarga esté completa. El sistema mantiene una memoria caché (*cache memory*) de archivos descargados recientemente, y cuando los mismos se solicitan de nuevo, los recupera inmediatamente. La cola de descarga se ordena según el tamaño del archivo, por lo tanto los archivos pequeños se descargan primero.

Como una parte del ancho de banda se dedica para este sistema aún en las horas pico, los usuarios que soliciten archivos pequeños pueden recibirlos en minutos, algunas veces hasta más rápido que una descarga en línea.

- Otro enfoque puede ser crear una interfaz web donde los usuarios ingresen el URL del archivo que quieran descargar. El mismo se descarga durante la noche utilizando una tarea programada (*cron job*, en inglés). Este sistema funciona solamente para usuarios que no sean impacientes, y que estén familiarizados con los tamaños de archivos que pueden ser problemáticos para descargar durante las horas de trabajo.

Envío de archivos pesados

Cuando los usuarios necesitan transferir archivos grandes a colaboradores en cualquier lugar en Internet, se les debe enseñar cómo programar la carga (*upload*) del archivo. En Windows, cargar archivos a un servidor FTP remoto puede hacerse utilizando un guión (*script*) FTP, que es un archivo de texto con comandos FTP.

Usuarios enviándose archivos unos a otros

Los usuarios a menudo necesitan enviarse archivos grandes. Si el receptor es local, es un gasto innecesario de ancho de banda enviarlos vía Internet. Para eso se debe crear un recurso compartido en el servidor web local Windows / Samba / Mac, donde un usuario puede colocar archivos grandes para que otros los descarguen. Como una alternativa, puede escribirse una interfaz web para que un servidor web local acepte un archivo pesado y lo coloque en un área de descarga. Después de cargarlo al servidor web, el usuario recibe un URL correspondiente al archivo, que puede transmitir a sus colaboradores locales o internacionales para que accedan al archivo. Esto es lo que ha hecho la Universidad de Bristol con su sistema FLUFF. La universidad ofrece una facilidad para la carga de archivos pesados (FLUFF por su sigla en inglés) disponible en *http://www.bris.ac.uk/it-services/applications/fluff/*.

Hay otras herramientas como SparkleShare (http://sparkleshare.org/) y Lipsync (https://github.com/philcryer/lipsync) que cumplen más o menos

la misma función y que son paquetes de fuente abierta que los puede instalar y configurar usted mismo(a). También hay servicios en línea gratuitos como Google Drive que puede instalarse para compartir archivos y ediciones sencillas.

Considere el uso de **rsync** (http://rsync.samba.org/) para el caso de los usuarios que tengan que mandarse frecuentemente entre ellos los mismos (o similares) archivos de gran tamaño.
El protocolo Rsync es una sincronización más bien que un protocolo directo de transferencia de archivos. En lugar de simplemente mandar un archivo desde el comienzo hasta el final, chequea con un servidos rsync en la computadora destinataria para comprobar si el archivo ya existe. Si existe, ambas máquinas comparan sus respectivas copias y la remitente transmite al destino solamente lo que sea diferente.
Por ejemplo, si una base de datos de investigación de 10 MB tiene solamente 23 KB de datos nuevos cuando se compara con la versión anterior, se transmitirán solamente esos 23 KB de cambios.
Rsync puede también usar el protocolo SSH para proporcionar una capa de transporte segura para las acciones sync.

Seguimiento e informe de problemas

La detección de problemas es sólo la mitad de la tarea de resolución de problemas de una red inalámbrica. Una vez diagnosticado y arreglado un problema, hay que documentarlo de manera permanente, de manera que otras personas que trabajen en esa red sepan qué hacer en el futuro o puedan aprender la lección a partir de esa ese incidente.
Llevar un registro de problemas e incidentes que ya han ocurrido es también una forma de hacer seguimiento y resolución de problemas a largo plazo que se presenten con regularidad, por ejemplo, cada cierto número de meses, y que tengan un patrón de comportamiento definido.
Se puede reducir la complejidad y la frustración de la detección de un problema si lleva un diario de cada cambio que se ha hecho en la red.
El diario o registro es donde usted y su equipo van a consignar por escrito cada cambio hecho en el sistema junto con la fecha y la hora en que se hizo ese cambio. Por ejemplo:

23 July 10:15AM Changed default route on host alpha from 123.45.67.89 to 123.56.78.1 because upstream ISP moved our gateway.

A medida del crecimiento de su red debe pensar en la instalación de sistemas de diagnóstico de problemas como JIRA o Bugzilla para ayudar a detectar quién está trabajando en cuál problema y qué ha pasado durante ese trabajo. Esto permite elaborar una historia de cuál problema específico se trató y de cómo se arregló, con lo que se construye un método ordenado de asignación de tareas y de prevención de situaciones como la de dos personas tratando al mismo tiempo de resolver el mismo problema y obstaculizándose mutuamente el trabajo.

Los sistemas de *trouble-ticketing* son un tema que llenaría otro libro. Lo mencionamos solamente para que se tengan en cuenta. Estos sistemas pueden ser complicados de implementar, por lo que para redes sencillas, llevar un diario será suficiente.

16. MONITOREO DE LA RED

Introducción

El monitoreo de la red es el uso de registro (*logging*) y herramientas de análisis para determinar con precisión el flujo de tráfico, la utilización y otros indicadores de desempeño característicos de una red.

Unas herramientas buenas para monitoreo le proporcionan cifras numéricas y representaciones gráficas del estado de la red.
Esto le va a ayudar a visualizar en detalle lo que está ocurriendo, de manera que sepa cuáles son los ajustes que necesita hacer.

Estas herramientas le ayudarán a responder preguntas básicas, como las siguientes:

- ¿Cuáles son los servicios más populares usados en la red?
- ¿Quiénes hacen uso más intenso de la red?
- ¿Qué otros canales inalámbricos se usan en el área?
- ¿Hay usuarios que estén instalando puntos de acceso inalámbricos en mi red cableada de uso privado?
- ¿A que hora del día es más utilizada la red?
- ¿Cuáles son los sitios más visitados por sus usuarios?
- ¿Está el tráfico entrante y saliente cerca de la capacidad disponible de nuestra red?
- ¿Hay indicaciones de alguna situación inusual en la red que esté consumiendo ancho de banda o causando otros problemas?
- ¿El Proveedor de Servicios de Internet (ISP) está dándonos el servicio por el que estamos pagando? Esto debe responderse en términos de ancho de banda disponible, pérdida de paquetes, latencia, y disponibilidad general.

Esto debería responderse en términos de ancho de banda disponible, pérdidas de paquetes, latencia y disponibilidad general.

Y tal vez, la pregunta más importante de todas:

- ¿El patrón de tráfico observado cumple con nuestras expectativas?

Las herramientas de medición y monitoreo son programas de importancia vital que hay que tener a mano para controlar la salud de la red y diagnosticar/resolver problemas.
En capítulos anteriores hemos dado ejemplos breves de cómo usar ciertas herramientas para tareas específicas como configuración y montaje, resolución de problemas, recolección de datos estadísticos y de mediciones sobre la salud de su red.
En esta sección se discuten algunas de esas herramientas en más detalle. Debe considerarse, sin embargo, que esta no es una lista exhaustiva de todas las herramientas existentes para redes cableadas o inalámbricas.
También es importante darse cuenta de que las herramientas de diagnóstico y monitoreo cambian al igual que otros tipos de software y hardware. Mantenerse actualizado con las últimas versiones, los bugs de las versiones existentes, nuevas herramientas en el campo, etc., puede ser en sí mismo un trabajo a tiempo completo. Para este libro, cuando hemos encontrado alguna herramienta que ha sido descontinuada entre la anterior edición y la actual, la hemos eliminado del texto. Las que se incluyen en la presente edición están en desarrollo para el momento de la escritura de esta nueva edición, pero se deja como ejercicio para el/la lector/a determinar si una herramienta determinada se adecua a su caso particular.

Ejemplo de monitoreo de red

Examinemos cómo un administrador típico de un sistema puede hacer un buen uso de las herramientas de monitoreo de red.

Un ejemplo efectivo

Para dar un ejemplo, vamos a suponer que estamos encargados de una red que ha estado funcionando por tres meses. Consiste de 50 computadoras y tres servidores: servidores de correo, web y proxy.

Mientras que al comienzo las cosas van bien, los usuarios comienzan a quejarse de la lentitud de la red y del aumento de spam. A medida que pasa el tiempo, el desempeño se hace mucho más lento (incluso cuando no se usa la red), lo que causa gran frustración a los usuarios.

Debido a las quejas frecuentes y al poco uso de las computadoras, el Consejo de administración se pregunta si hay necesidad de tanto hardware para la red. También quieren tener la seguridad de que el ancho de banda que están pagando se está usando efectivamente.

En tanto administrador/a de la red, usted es quien recibe todas las quejas. ¿Cómo hace usted para diagnosticar la caída repentina de la red y el bajo desempeño de las computadoras, y a la vez, justificar los costos de hardware y ancho de banda?

Monitoreo de LAN (tráfico local)

Para tener una idea de qué es exactamente lo que está causando el enlentecimiento, usted debería comenzar por examinar el tráfico en la LAN local. Hay varias ventajas en hacer esto:

1. La resolución de problemas se simplifica bastante.
2. Los virus pueden ser localizados y eliminados
3. Los usuarios intrusos pueden detectarse y se puede solucionar el problema
4. Los recursos y el hardware de la red pueden justificarse con estadísticas reales.

Suponga que todos los conmutadores (*switches*) utilizan ***SNMP (Simple Network Management Protocol).*** SNMP es un protocolo de la capa de aplicaciones diseñado para facilitar el intercambio de información de gestión entre los dispositivos de la red. AL asignarle una dirección IP a cada conmutador, será capaz de monitorear todas las interfaces en ese conmutador y observar la red entera desde un sólo punto. Esto es mucho más fácil que habilitar SNMP en todas las computadoras de la red.

Usando una herramienta gratuita como MRTG (http://oss.oetiker.ch/mrtg), se puede monitorear cada puerto en el conmutador y presentar los datos gráficamente, como un promedio acumulado en el tiempo. Las gráficas están disponibles en la web, de manera que puede verlas desde cualquier máquina en cualquier momento.

Mediante monitoreo MRTG, es obvio que la LAN interna está inundada con mucho más tráfico de lo que la conexión Internet puede manejar, incluso cuando el laboratorio no está ocupado.
Esto es una indicación clara de que algunas computadoras están infestadas de virus.
Luego de instalar un buen programa antivirus y detector de *spyware* en todas las máquinas, el tráfico de la LAN interna baja a los niveles esperados. Las máquinas funcionan más rápidamente, se reducen los correos spam, y el ánimo de los usuarios mejora también rápidamente.

Monitoreo de WAN (tráfico externo)

Además de supervisar el tráfico de la LAN interna, usted necesita demostrar que el ancho de banda que la organización está pagando es el que de verdad están obteniendo de su ISP. Esto puede lograrlo al monitorear el tráfico externo. El tráfico externo se clasifica generalmente como todo aquello que se envía por una Red de Área Extendida, WAN (*Wide Area Network*). Todo lo que se reciba desde (o se envíe a) una red diferente a su LAN interna, también califica de tráfico externo. Las ventajas de monitorear el tráfico externo incluyen:

1. Los costos de ancho de banda de Internet pueden justificarse mostrando su uso real y comparándolo con lo que su ISP le está cobrando por el ancho de banda.
2. Las necesidades futuras de capacidad pueden calcularse examinado las tendencias de uso y prediciendo patrones de crecimiento probables.
3. Los intrusos provenientes de Internet se detectan y se filtran antes de que causen problemas.

Monitorear el tráfico es tarea fácil con el uso de MRTG en un dispositivo habilitado con SNMP, como por ejemplo un enrutador.

Si su enrutador no soporta SNMP, entonces puede añadir un conmutador entre el enrutador y la conexión de su ISP, y monitorear el tráfico del puerto como lo haría con una LAN interna.

Cómo detectar apagones de red

Con las herramientas de monitoreo en su sitio, usted tiene ahora una medida precisa de cuánto ancho de banda está usando su organización.
Esta medida debería concordar con lo que está cobrando su ISP por el ancho de banda.
Puede también indicarle el caudal (*throughput*) real de su conexión si usted está cerca del límite de su capacidad disponible en horas pico.
Una traza de tráfico con una línea horizontal en la parte superior es una indicación clara de que usted está operando a su máxima capacidad.
La figura MR 1 muestra esta "línea plana" para el tráfico de salida pico al mediodía, de cada día, excepto los domingos.

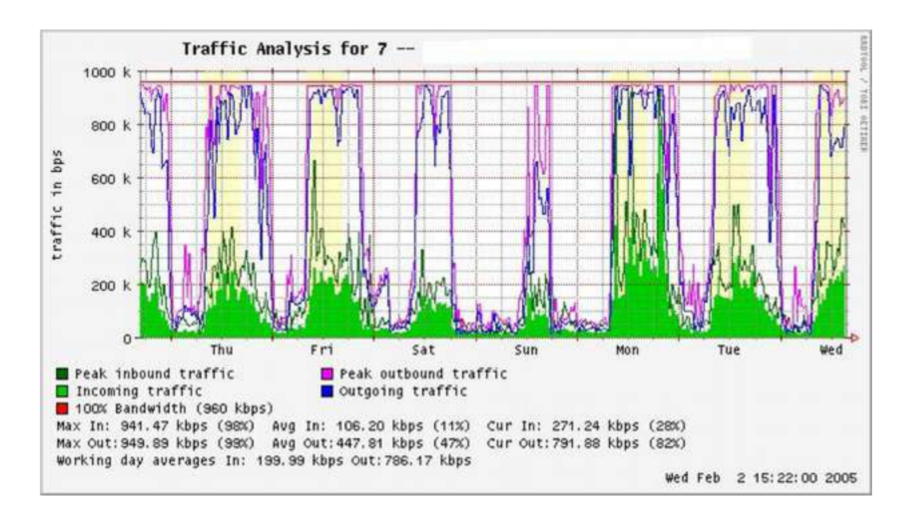


Figura MR 1: Una gráfica de traza plana en el tope indica sobreutilización

Más tarde en la semana, usted recibe una llamada telefónica de emergencia en la tarde. Aparentemente, nadie en el laboratorio puede navegar en la web o mandar correos. Usted corre al laboratorio y rápidamente reinicializa el servidor proxy, sin resultados. Ni la web ni los correos funcionan. Reinicializa el enrutador, pero todavía sin éxito. Continúa eliminando una a una las posibles áreas problemáticas hasta que se da cuenta de que el conmutador de la red está apagado: un cable de energía suelto es el culpable. Después de conectar, la red vuelve a la vida

.¿Cómo se puede detectar este tipo de falla sin emplear este largo proceso de ensayo y error? ¿Es posible tener notificación de fallas en el momento en que se producen, en lugar de esperar las quejas de los usuarios? Una forma de lograrlo es usando un programa como **Nagios** (http://www.nagios.org) que continuamente examina los dispositivos de la red y le notifica las fallas. Nagios le va a informar sobre la disponibilidad de las diferentes máquinas y sus servicios y le alertará sobre las máquinas que están fallando. Además de presentarle el estatus de la red gráficamente en una página web, le enviará notificación por SMS o email para alertarle en el momento en que se produce el problema.

Con las herramientas de monitoreo en su lugar, usted debería ser capaz de justificar los costos de equipamiento y banda ancha demostrando efectivamente cómo es utilizada la red por la organización.

Usted es notificado/a en el momento preciso en que surgen los problemas y tiene una historia estadística del rendimiento de los diferentes dispositivos. Puede comprobar los problemas presentes por comparación con el registro histórico para detectar comportamiento anómalo, y atacar los problemas antes de que se agraven. Si el problema se presenta de todas maneras, es más fácil determinar su fuente y naturaleza. Su trabajo es más fácil, el Consejo queda satisfecho y los usuarios están más contentos.

Monitoreo de su red

Administrar una red sin monitorearla es equivalente a manejar un vehículo sin un velocímetro, o sin medidor de gasolina y con los ojos cerrados. ¿Cómo hace para saber a qué velocidad conduce? ¿El vehículo está consumiendo combustible de manera tan eficiente como le prometió el vendedor? Si usted le hace mantenimiento al vehículo unos meses después, ¿va a tener más velocidad o a ser más eficiente que antes? De manera semejante, ¿cómo puede usted pagar el recibo del agua o de la electricidad en su casa sin ver en el medidor cuánto es su consumo mensual? En su red, usted debe llevar cuenta de la utilización del ancho de banda para poder justificar los costos de los servicios y de las compras de hardware y para dar cuenta de las tendencias de uso. Hay varios beneficios al implementar un buen sistema para monitorear su red:

- Los recursos y el presupuesto de red pueden justificarse.
  Buenas herramientas de monitoreo pueden demostrar sin lugar a dudas que la infraestructura de red (ancho de banda, hardware y software) es adecuada y capaz de manejar las necesidades de los usuarios de la red.

- Los intrusos de la red pueden detectarse y filtrarse. Al supervisar el tráfico de su red, puede detectar a los atacantes e impedirles el acceso a los servidores y servicios de la red.

- La resolución de problemas en la red se simplifica mucho. En vez de emplear el método de ensayo y error, para eliminar los problemas usted recibe notificación instantánea sobre un problema específico. Algunas de las fallas pueden incluso ser reparadas automáticamente.

- El rendimiento de la red puede ser optimizado en gran medida. Sin un monitoreo efectivo, es imposible afinar el funcionamiento de sus dispositivos y protocolos para lograr el mayor rendimiento posible.

- La planificación de capacidad es más fácil. Con registros cronológicos sólidos sobre desempeño, usted no tendrá que "adivinar" cuánto ancho de banda va a necesitar su red cuando ésta crezca.

- El uso apropiado de la red puede hacerse valer. Cuando el ancho de banda es un recurso escaso, la única forma de ser justos con los usuarios es asegurarse de que la red se usa para lo que fue creada.

Afortunadamente, el monitoreo de la red no necesita ser una labor costosa. Hay numerosas herramientas de fuente abierta gratuitas que le enseña lo que está pasando exactamente en su red con bastantes detalles. Esta sección va a ayudarle a identificar muchas herramientas valiosas y a enseñarle la mejor manera de usarlas.

El servidor de monitoreo dedicado

Aunque hay herramientas de monitoreo que pueden adicionarse a un servidor de red ya existente, es deseable dedicar una máquina (o más, si fuera necesario) al monitoreo de la red. Algunas aplicaciones (como **ntop**: http://www.ntop.org) necesitan recursos considerables para ejecutarlas, especialmente en una red de mucho tráfico.
Pero la mayor parte de los programas de registro (logging) y de monitoreo tienen exigencias modestas de RAM y almacenamiento, y de potencia del CPU. Puesto que los sistemas operativos de fuente abierta (como Linux o BSD) hacen un uso muy eficiente de los recursos de hardware, esto hace que sea posible construir un servidor de monitoreo muy capaz, a partir de piezas de PC recicladas. Usualmente no hay necesidad de comprar un servidor nuevo para dedicarlo a las labores de monitoreo.

La excepción a esta regla son las instalaciones muy grandes. Si su red comprende más de unos cientos de nodos, o si usted consume más de 50 Mbps de ancho de banda de Internet, es probable que necesite dividir las labores de monitoreo entre varias máquinas dedicadas.
Esto va a depender mucho de lo que quiera monitorear exactamente.

Si usted quiere dar cuenta de todos los servicios accedidos a través de direcciones MAC, esto consumirá bastantes más recursos que la simple medición del flujo de tráfico en un puerto del conmutador.

Pero, para la mayoría de las instalaciones, una sola máquina dedicada es normalmente suficiente. Concentrar el monitoreo en una sóla máquina le permite agilizar la administración y las actualizaciones, y le garantiza una mejor continuidad del proceso de monitoreo.

Por ejemplo, si instala un servicio de monitoreo en un servidor web, y ese servidor presenta problemas, su red no puede ser monitoreada hasta tanto el problema haya sido resuelto. Para un/a administrador/a de red, los datos recogidos acerca del desempeño de la red son casi tan importantes como la red misma. Su monitoreo debe ser robusto y tan bien protegido contra fallas de energía como sea posible. Sin estadísticas de red, usted está ciego/a ante los problemas de la red.

¿Dónde encaja el servidor en su red?

Si su interés es sólo recoger estadísticas del flujo de la red de un enrutador, lo puede hacer desde casi cualquier sitio de la LAN. Esto le da una retroalimentación básica sobre utilización, pero no puede darle detalles amplios sobre patrones de uso. La Figura MR 2 muestra una gráfica típica MRTG generada desde el enrutador a Internet. Mientras que se distingue claramente el tráfico entrante y saliente, no hay detalles sobre cuáles computadoras, usuarios o protocolos están usando ancho de banda.

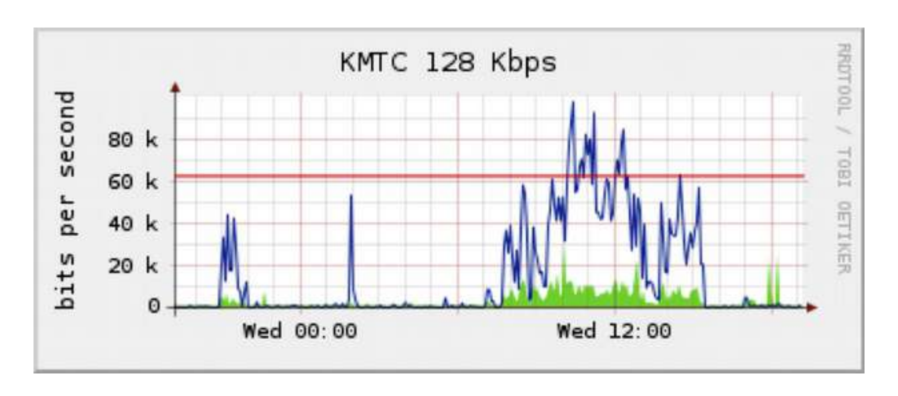


Figura MR 2: Sondear el enrutador perimétrico puede mostrarle la utilización general de la red, pero los datos no pueden analizarse en términos de máquinas, servicios y usuarios

Para más detalles, el servidor dedicado al monitoreo debe tener acceso a todo lo que se necesite supervisar. Usualmente, esto significa que debe tener acceso a la red completa. Para monitorear una conexión WAN, como el enlace Internet hacia su ISP, el servidor de monitoreo debe ser capaz de ver el tráfico que pasa por el enrutador perimetral.
Para monitorear una LAN, el servidor está comúnmente conectado con un **puerto monitor** en el conmutador. Si se están usando varios conmutadores en una instalación, el servidor monitor podría necesitar una conexión con todos ellos. Esta conexión puede ser un cable real, o si los conmutadores de su red lo permiten, una VLAN configurada específicamente para monitoreo de tráfico.

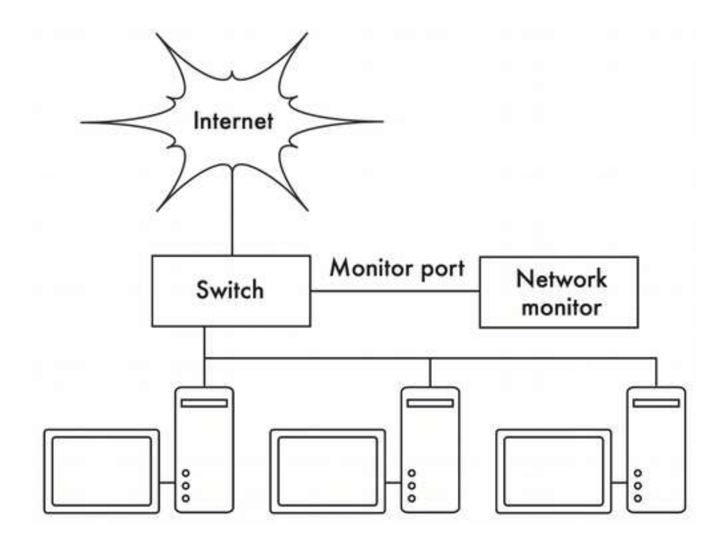


Figura MR 3: Use el puerto monitor en su conmutador para observar el tráfico que cruza todos los puertos de la red

Si la función de puerto monitor no está disponible en su conmutador, el servidor monitor podría instalarse entre su LAN interna e Internet.

A pesar de que esto funciona, introduce una falla crucial en la red, ya que esta fallará si el servidor monitor presenta algún problema.
También pudiera ser una fuente de embotellamiento si el servidor se ve incapacitado de cumplir las exigencias de la red.

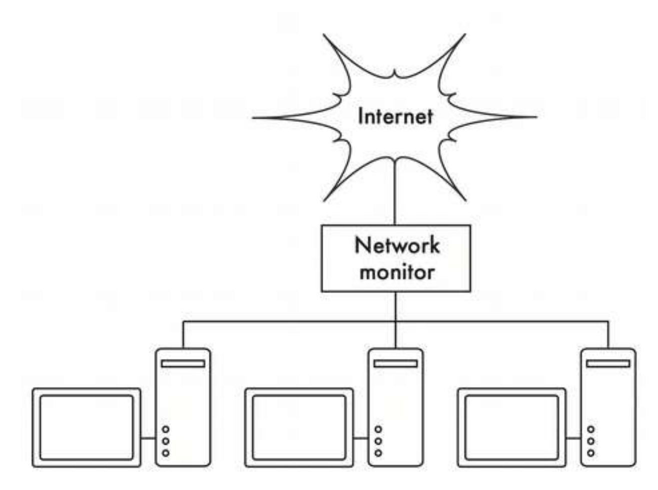


Figura MR 4: Al insertar un monitor de red entre la LAN y su conexión a Internet se puede observar todo el tráfico de la red

Una solución mejor es la de usar un simple (*hub*) concentrador de red (no un conmutador) que conecte la máquina monitora con la LAN interna, el enrutador externo y la máquina monitora. A pesar de que esto todavía introduce un punto adicional de falla en la red (puesto que la red completa será inaccesible si el concentrador se "muere"), los concentradores son considerados más confiables que los enrutadores. También son más fácilmente reemplazables si fallan.

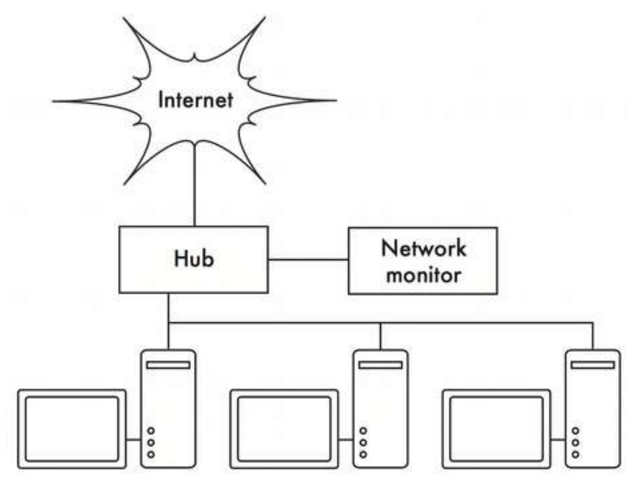


Figura MR 5: Si su conmutador no tiene la funcionalidad de puerto monitor, puede insertar un concentrador de red entre el enrutador de Internet y la LAN, y conectar el servidor monitor al concentrador

Con el servidor de monitoreo en su lugar, ya estamos listos para recolectar los datos.

¿Qué debemos monitorear?

Es posible graficar casi cualquier evento de red y observar su valor en el tiempo.
Ya que cada red es ligeramente diferente, usted tendrá que decidir cuál es la información importante con el fin de calibrar el rendimiento de su red. Aquí les presentamos algunos indicadores importantes que un/una administrador/a de red comúnmente investiga:

Estadísticas de la red inalámbrica

- Señal y ruido recibidos desde todos los nodos del backbone
- Número de estaciones asociadas
- Redes y canales adyacentes detectados
- Retransmisiones excesivas
- Tasa de datos en los radios, si usa adaptación automática

Estadísticas del conmutador

- Uso de ancho de banda por puerto del conmutador
- Uso de ancho de banda discriminado por protocolo
- Uso de ancho de banda discriminado por direcciones MAC
- Porcentaje de paquetes de difusión respecto al total
- Pérdida de paquetes y tasa de error

Estadísticas de Internet

- Uso de ancho de banda por anfitrión y por protocolo
- Solicitudes a la caché del servidor proxy
- Los 100 sitios más visitados
- Solicitudes de DNS
- Número de correos entrantes, correos spam, correos rebotados
- Tamaño de la cola de correos entrantes
- Disponibilidad de servicios críticos (servidores web, servidores de correo, etc.)
- Tiempos ping y tasa de pérdida de paquetes a su ISP
- Estatus de los respaldos

Estadísticas de la salud del sistema

- Uso de memoria
- Uso del archivo Swap
- Conteo de procesos / Procesos zombie
- Carga del sistema Voltaje y carga del UPS
- Temperatura, velocidad del ventilador y voltajes del sistema
- Estatus del SMART del disco
- Estatus del arreglo RAID

Esta lista debería usarse como una sugerencia de dónde comenzar. A medida que su red madure, es probable que usted encuentre nuevos indicadores del rendimiento de su red y, por supuesto, debería analizarlos también. Hay muchas herramientas gratuitas disponibles que van a darle tantos detalles como desee sobre lo que pasa en su red. Usted debería considerar el monitoreo de la disponibilidad de cualquier recurso cuando la no-disponibilidad pueda afectar negativamente a los usuarios.

No olvide monitorear la máquina monitora misma, por ejemplo el uso de la CPU y el espacio de disco para recibir advertencias por adelantado si se sobrecarga o falla. Una máquina monitora que tiene pocos recursos puede afectar su capacidad de monitorear la red efectivamente.

Tipos de herramientas de monitoreo

Veamos ahora varios tipos diferentes de herramientas de monitoreo:

1. Las herramientas de detección de red interpretan las balizas (*beacons)* enviadas por los puntos de acceso inalámbricos y presentan información como el nombre de la red, intensidad de la señal recibida, y canal.

2. Las herramientas de monitoreo puntual están diseñadas para resolución de problemas y suelen funcionar interactivamente por períodos cortos. Un programa como **ping** puede considerarse como una herramienta de monitoreo puntual activa, puesto que genera tráfico sondeando a una máquina específica.

3. Las herramientas de monitoreo puntual pasivas incluyen analizadores de protocolo, que inspeccionan cada paquete de la red y proporcionan detalles completos sobre cualquier conversación de red (incluido direcciones de fuente y destino, información de protocolo, e incluso datos de aplicación).

4. Las herramientas de predicción realizan monitoreo sin supervisión por períodos largos, y comúnmente presentan los resultados en una gráfica.

5. Las herramientas de medida de caudal informan sobre el ancho de banda real disponible entre dos puntos en la red.

6. Las herramientas de monitoreo en tiempo real hacen un monitoreo similar, pero le avisan al/la administrador/a cuando detectan un problema. Las herramientas de detección de intrusos supervisan el tráfico indeseable o inesperado y toman las medidas apropiadas (normalmente denegando acceso y/o notificando al/la administrador/a).

Detección de redes

Las herramientas de monitoreo comunes, simplemente proveen una lista de redes disponibles con información básica (tales como intensidad de la señal y canal). Le permiten detectar rápidamente redes cercanas y determinar si están dentro de su alcance o si están causando interferencia.

Las incorporadas en el cliente

Todos los sistemas operativos modernos proveen soporte incorporado para redes inalámbricas. En general este incluye la habilidad de explorar en búsqueda de redes disponibles, permitiéndole al usuario elegir una red de la lista. Si bien prácticamente todos los dispositivos inalámbricos incluyen una utilidad simple de exploración, las funcionalidades puede variar ampliamente entre implementaciones. En general, son útiles solamente para configurar una computadora en su hogar o en la oficina. Tienden a proveer poca información más allá de los nombres de las redes y la intensidad de señal recibida desde el punto de acceso en uso.

Netstumbler

(http://www.wirelessdefence.org/Contents/NetstumblerMain.htm). Es la herramienta más popular para detectar redes inalámbricas utilizando Microsoft Windows. Respalda una variedad de tarjetas inalámbricas, y es muy sencilla de utilizar. Detecta redes abiertas y encriptadas, pero no puede detectar redes inalámbricas "cerradas". También ofrece un medidor de señal/ruido que grafica la señal recibida a lo largo del tiempo. También se puede integrar con una variedad de dispositivos GPS, para registrar ubicaciones precisas e información sobre la potencia de la señal.

Todo esto hace que Netstumbler sea una herramienta accesible para realizar una prospección informal de la zona.

Macstumbler (http://www.macstumbler.com/). Si bien no está relacionado directamente con Netstumbler, Macstumbler brinda muchas de sus funcionalidades pero para la plataforma Mac OS X. Funciona con todas las tarjetas Apple Airport.

Herramientas de monitoreo puntual

¿Qué hace cuando la red se daña? Si no puede acceder a una página web o a un servidor de correo electrónico, y el problema no se soluciona presionando el botón de “actualizar”, se hace necesario aislar la ubicación exacta del problema.

Las herramientas siguientes, a manera de introducción, lo van a ayudar a determinar dónde se encuentra el problema. Para más detalles vea el capítulo **Mantenimiento y Soluciones**.

ping. Casi todos los sistemas operativos (incluyendo Windows, Mac OS X, y por supuesto Linux y BSD) incluyen una versión de la utilidad *ping*. Utiliza paquetes ICMP para intentar contactar un servidor específico y le informa cuánto tiempo lleva obtener una respuesta.

Saber a quién dirigir el *ping* es tan importante como saber cómo hacerlo. Si usted no puede conectarse a un servicio en su navegador web (por ejemplo, http://yahoo.com/), puede intentar contactarlo con ping:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Presione control-C cuando haya terminado de colectar datos.

Si los paquetes se toman mucho tiempo en regresar, puede haber una congestión en la red. Si los paquetes ping de retorno tienen un TTL (*Time to Live*) inusualmente bajo, puede que haya problemas de enrutamiento entre su computadora y el extremo remoto. ¿Pero, qué sucede si *ping* no obtiene respuesta? Si está haciendo ping a un nombre en lugar de una dirección IP, puede que tenga problemas de DNS. Intente contactar una dirección IP en Internet. Si no puede acceder a ella, es una buena idea observar si puede contactar su enrutador por defecto:

```
$ ping 69.90.235.230

PING 69.90.235.230 (69.90.235.230): 56 data bytes

64 bytes from 69.90.235.230: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 69.90.235.230: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 69.90.235.230: icmp_seq=2 ttl=126 time=13.897 ms
^C

--- 216.231.38.1 ping statistics ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms
```

Si no puede contactar a su enrutador por defecto, entonces lo más probable es que tampoco pueda acceder a Internet. Si tampoco puede contactar otras direcciones IP en su LAN local, es tiempo de verificar su conexión. Si está utilizando cable Ethernet, ¿está enchufado? Si está utilizando una conexión inalámbrica, ¿esta usted conectado a la red correcta, y está la red dentro del rango de cobertura?

Generalmente es acertado suponer que una máquina que no responde a un ping está caída o desconectada de la red; pero no siempre se cumple en el 100% de los casos. En una WAN en particular, o en la misma Internet es también posible que algún enrutador/cortafuegos entre usted y el anfitrión-objetivo (o el mismo anfitrión) esté bloqueando los pings. Si tiene alguna máquina que no responde a los pings, pruebe otros servicios bien conocidas como ssh o http.

Si puede alcanzar el objetivo por medio de estos servicios, quiere decir que su máquina está bien, sólo que está bloqueando los pings. Hay que hacer notar que los diferentes sistemas van a tratar ping de diferente manera. La utilidad clásica ping de UNIX envía un paquete de protocolo ICMP ECHO al anfitrión objetivo. Otros dispositivos de red, en cambio, responderán al ping automáticamente pese a que ICMP esté bloqueado más adelante en la pila de protocolos.
Esto puede confundirnos porque podría interpretarse como que un anfitrión está respondiendo cuando en verdad lo que sucede es que la tarjeta de interfaz de red NIC (Network Interface Card) está encendida, pero la máquina en sí misma no está dando respuesta.
Como ya dijimos, es siempre bueno chequear la conectividad por múltiples métodos. El diagnóstico de problemas de la red con ping es casi un arte; sin embargo, vale la pena aprenderlo. Puesto que en casi toda máquina en la que trabaje va a encontrar ping, es buena idea aprender a usarlo bien.
traceroute y **mtr**

http://www.bitwizard.nl/mtr/

Como sucede con **ping, traceroute** está en la mayoría de los sistemas operativos (en algunas versiones de Microsoft Windows se le denomina **tracert**). Si ejecuta traceroute, puede rastrear la ubicación de los problemas entre su computadora y cualquier punto en Internet:

$ traceroute -n google.com

traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets

1 10.15.6.1 4.322 ms 1.763 ms 1.731 ms

2 216.231.38.1 36.187 ms 14.648 ms 13.561 ms

3 69.17.83.233 14.197 ms 13.256 ms 13.267 ms

4 69.17.83.150 32.478 ms 29.545 ms 27.494 ms

5 198.32.176.31 40.788 ms 28.160 ms 28.115 ms

6 66.249.94.14 28.601 ms 29.913 ms 28.811 ms

7 172.16.236.8 2328.809 ms 2528.944 ms 2428.719 ms

*8 * * **

La opción **-n** le dice a **traceroute** que no se preocupe por resolver los

nombres en el DNS, permitiendo que el programa se ejecute más rápido. Usted puede ver que en el salto siete, el tiempo de recorrido de ida y vuelta se dispara a más de dos segundos, mientras que los paquetes parece que se descartan en el salto ocho. Esto puede indicar un problema en ese punto de la red. Si esta parte de la red está bajo su control, vale la pena comenzar por ahí sus esfuerzos para resolver el problema.

My TraceRoute (**mtr**) es un programa que combina **ping y traceroute** en una sola herramienta. Al ejecutar **mtr**, se puede obtener un promedio de la latencia y la pérdida de paquetes hacia un servidor en cierto lapso, en lugar de la visión instantánea que ofrecen ping y traceroute.

My traceroute [v0.69]

tesla.rob.swn (0.0.0.0) (tos=0x0 psize=64 bitpat Sun Jan 8 20:01:26 2006)

Keys: Help Display mode Restart statistics Order of fields quit

Packets			***Pings***				
Host	***Loss%***	***Snt***	***Last***	***Avg***	***Best***	***Wrst***	***StDev***
1. gremlin.rob.swn	*0.0%*	*4*	*1.9*	*2.0*	*1.7*	*2.6*	*0.4*
2. er1.sea1.speakeasy.net	*0.0%*	*4*	*15.5*	*14.0*	*12.7*	*15.5*	*1.3*
3. 220.ge-0-1-0.cr2.sea1. Speakeasy.net	*0.0%*	*4*	*11.0*	*11.7*	*10.7*	*14.0*	*1.6*
4. fe-0-3-0.cr2.sfo1. speakeasy.net	*0.0%*	*4*	*36.0*	*34.7*	*28.7*	*38.1*	*4.1*
5. bas1-m.pao.yahoo.com	*0.0%*	*4*	*27.9*	*29.6*	*27.9*	*33.0*	*2.4*
6. so-1-1-0.pat1.dce. yahoo.com	*0.0%*	*4*	*89.7*	*91.0*	*89.7*	*93.0*	*1.4*
7. ae1.p400.msr1.dcn. yahoo.com	*0.0%*	*4*	*91.2*	*93.1*	*90.8*	*99.2*	*4.1*
8. ge5-2.bas1-m.dcn. yahoo.com	*0.0%*	*4*	*89.3*	*91.0*	*89.3*	*93.4*	*1.9*
9.w2.rc.vip.dcn.yahoo.com	*0.0%*	*3*	*91.2*	*93.1*	*90.8*	*99.2*	*4.1*

Los datos van a ser actualizados y promediados continuamente.

Al igual que con *ping*, cuando haya terminado de observar los datos debe presionar control-C. Tenga en cuenta que para usar **mtr** debe tener privilegios de administrador (root).

Si bien estas herramientas no van a revelar exactamente qué es lo que está funcionando mal en una red, pueden darle información suficiente para saber por dónde continuar en la resolución de problemas.

Analizadores de protocolos

Los analizadores de protocolos de redes proporcionan una gran cantidad de detalles de la información que fluye por una red, permitiendo inspeccionar paquetes individualmente. Para las redes cableadas, usted puede inspeccionar paquetes en la capa de enlace de datos o en una superior. Para el caso de las redes inalámbricas, se puede inspeccionar información hasta las tramas 802.11.

Aquí hay varios analizadores populares (y gratuitos) de protocolos de redes:

Kismet

http://www.kismetwireless.net/

Kismet es un poderoso analizador de protocolos inalámbrico para Linux, Mac OS X, y la distribución Linux embebida OpenWRT. Funciona con cualquier tarjeta inalámbrica que respalde el modo monitor pasivo.

Además de la detección básica de redes, Kismet registra pasivamente todas las tramas 802.11 al disco o la red en el formato estándar PCAP, para su futuro análisis con herramientas como Ethereal.

Kismet también ofrece información asociada del cliente, información de identificación (*fingerprinting*) del AP, detección de Netstumbler, e integración de GPS.

Como es un monitor pasivo de la red también puede detectar redes inalámbricas “cerradas”, analizando el tráfico enviado por los clientes.

Se puede ejecutar Kismet en varias computadoras al mismo tiempo, y hacer que todas reporten a través de la red a una misma interfaz de usuario.

Esto permite realizar un monitoreo inalámbrico sobre grandes áreas, tales como un campus universitario o corporativo.

Como utiliza el modo de monitoreo pasivo de la tarjeta de radio, hace todo esto sin transmitir ningún dato. Kismet es una herramienta valiosa para el diagnóstico de problemas de redes inalámbricas.

KisMAC

http://kismac-ng.org

Desarrollado exclusivamente para la plataforma Mac OS X, KisMAC puede hacer mucho de lo que Kismet hace, pero con una interfaz gráfica Mac OS X muy elaborada. Es un escáner pasivo que registra datos en el disco, en un formato PCAP compatible con Wireshark.

Admite un rastreo pasivo con tarjetas AirportExtreme así como una variedad de tarjetas inalámbricas USB.

tcpdump

http://www.tcpdump.org/

tcpdump es una herramienta de línea de comando para el monitoreo de tráfico de red. No tiene los detalles cosméticos de **wireshark**, pero usa menos recursos.

Tcpdump puede captar y presentar toda la información de protocolo de red hasta la capa de enlace. Puede mostrar todos los encabezados de los paquetes y datos recibidos o sólo los paquetes que cumplan con un criterio determinado. Los paquetes captados con tcpdump pueden ser cargados en wireshark para realizar análisis y diagnósticos posteriores. Esto es muy útil cuando se quiere monitorear una interfaz o un sistema remoto y traerse un archivo hasta su máquina para analizarlo.

Tcpdump se halla disponible como herramienta estándar en los sistemas derivados de Unix (Linux, BSD, y Mac OS X).

Hay también una versión Windows llamada **WinDump** disponible en: *http://www.winpcap.org/winpdump/*

Wireshark

http://www.wireshark.org/. Antes conocido como **Ethereal, wireshark** es un analizador de protocolo de red gratuito para Unix y Windows.

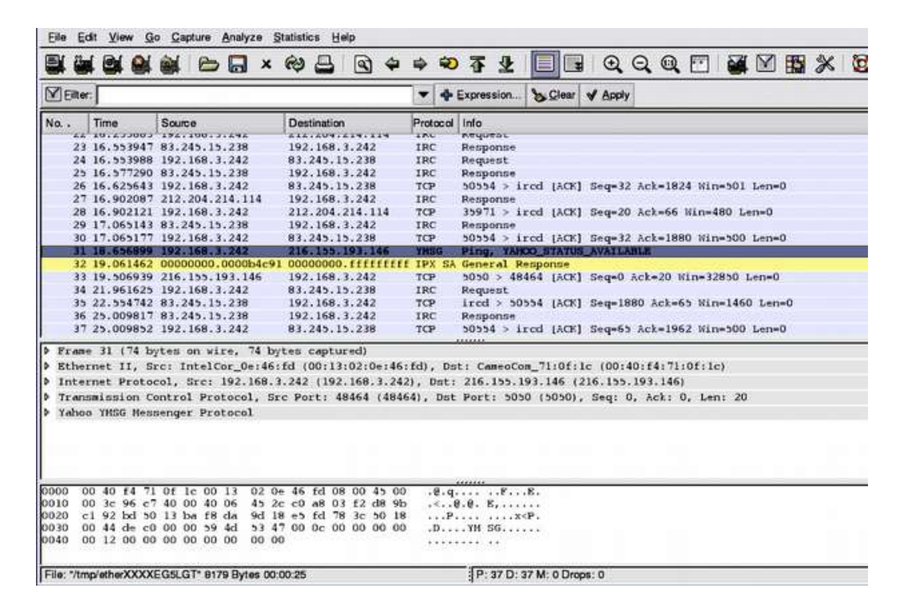


Figura MR 6: Wireshark (antes Ethereal) es un analizador de protocolo de red muy poderoso que puede mostrar todos los detalles que se deseen sobre los paquetes

Wireshark le permite examinar los datos de una red en vivo o de un archivo copiado desde un disco y examinar y clasificar los datos captados.

Tanto el resumen como la información detallada de cada paquete están disponibles, incluidos los encabezados completos y fragmentos de los datos.

Wireshark tiene algunas características muy poderosas, como un filtro de despliegue muy rico, y la capacidad de ver la cadena reconstruida de una sesión TCP.

Puede ser desalentador usarlo por primera vez o cuando las capas OSI no nos son familiares. Es comúnmente empleado para aislar y analizar tráfico específico desde o hacia una dirección IP, pero también puede usarse como una herramienta de uso general para detección de problemas.

Por ejemplo, una máquina infestada con un gusano o un virus puede detectarse buscando la máquina que envía el mismo tipo de paquetes TCP/IP a un gran número de direcciones IP.

Herramientas de predicción

Las herramientas de predicción se usan para ver cómo se está usando su red en un determinado período.

Funcionan monitorizando periódicamente la actividad de red y representándola de manera legible humanamente (gráficas, por ejemplo). Estas herramientas recolectan datos, los analizan y los presentan.

A continuación hay algunos ejemplos de herramientas de predicción. Algunas necesitan usarse en combinación con otras ya que no son programas independientes.

MRTG

http://oss.oetiker.ch./mrtg/

El ***Multi Router Traffic Grapher (MRTG)*** monitorea la carga de tráfico en enlaces de red usando SNMP. MRTG genera gráficas que dan una representación visual del tráfico entrante y saliente.

Estas gráficas se presentan normalmente en una página web. MRTG puede ser un poco confuso de instalar, especialmente si no se está familiarizado con SNMP.

Pero una vez instalado, MRTG virtualmente no requiere mantenimiento a menos que usted cambie algo en el sistema que se está monitoreando (como su dirección IP).

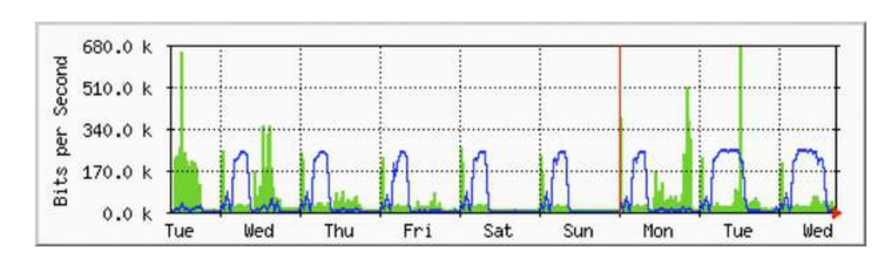


Figura MR 7: MRTG es probablemente el graficador de flujo instalado más a menudo

RRDtool

http://oss.oetiker.ch/rrdtool/

RDR es la sigla de ***Round Robin Database***. RDR es una base de datos que almacena información de manera muy compacta que no se expande con el tiempo. ***RRDtool*** se refiere a un conjunto de herramientas que permiten crear y modificar bases de datos RRD, así como generar gráficas útiles para representar los datos.

Se usa para mantener el registro de datos en series de tiempo (como ancho de banda de la red, temperatura del cuarto de máquinas, o promedio de carga del servidor), y puede presentar estos datos como un promedio en el tiempo.

Note que RRDtool, en sí mismo, no hace contacto con los dispositivos de red para recuperar los datos. Es meramente una herramienta de manipulación de bases de datos.

Puede usar simplemente un guión (*shell o Perl*, normalmente) para que haga este trabajo por usted. RRDtool es también utilizado por muchos *front-ends* (interfaz de usuario) con todas las funcionalidades que presentan una interfaz amigable para configuración y despliegue.

Las gráficas RRD le dan más control que MRTG sobre las opciones de presentación y número de elementos disponibles en la gráfica.

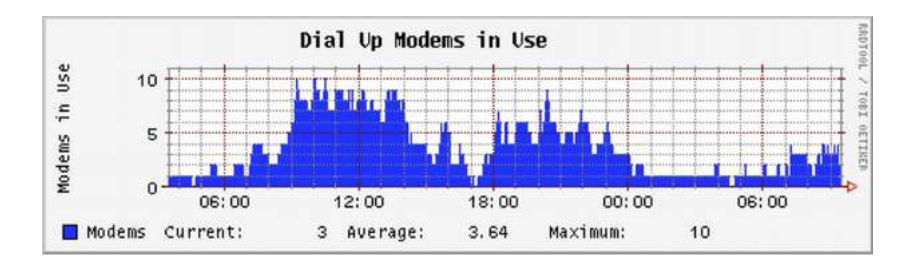


Figura MR 8: RRDtool le da mucha flexibilidad en cuanto a la forma de presentar los datos de red recolectados

RRDtool ya forma parte de todas las distribuciones de Linux modernas y puede descargarse desde http://oss.oetiker.ch/rrdtool/

ntop

http://www.ntop.org

Para el análisis histórico de tráfico y uso, considere **ntop**.

Este programa elabora un informe detallado en tiempo real sobre el tráfico de red observado y presentado en su navegador web.

Se integra con rrdtool y elabora gráficas y diagramas que describen visualmente cómo se está usando la red. En redes de mucho tráfico ntop puede usar mucho CPU y espacio de disco, pero le ofrece una buena visión sobre el uso de su red.

Funciona con Linux, BSD, Mac OS X, y Windows.

Algunas de sus características más útiles son:

La presentación del tráfico puede clasificarse de diversas maneras (fuente, destino, protocolo, direcciones MAC, etc.).

Las estadísticas de tráfico están agrupadas por protocolo y número de puerto

Una matriz de tráfico IP que muestra las conexiones entre máquinas. Flujos de red para enrutadores y conmutadores que utilizan el protocolo NetFlow. Identificación del sistema operativo del anfitrión. Identificación del tráfico P2P. Múltiples cuadros de gráficas. API Perl, PHP, y Python.

Ntop se puede descargar de *http://www.ntop.org/* y hay versiones para la mayoría de los sistemas operativos.

A menudo se incluye en las distribuciones más populares como Red Hat, Debian, y Ubuntu.

Aunque puede dejarse funcionando para colectar datos históricos, hace un uso bastante intensivo de la CPU, dependiendo del tráfico observado.

Si lo va a utilizar por largos períodos debería estar pendiente del uso de CPU en la máquina de monitoreo.

Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Flows	Accumulated Percentage / Historical Protocol View
FTP	17.8 KB	53	0%
HTTP	40.8 MB	1,410	88.2%
DNS	543.8 KB	4,851	1.1%
NBios-IP	35.4 KB	391	0%
Mail	1.2 MB	166	2.5%
SNMP	0.1 KB	1	0%
NNTP	0.4 KB	4	0%
Gnutella	0.3 KB	2	0%
BitTorrent	18.0 KB	2	0%
Messenger	4.0 KB	3	0%
Other TCP/UDP-based Protocols	3.7 MB	6,129	7.9%
Accumulated View	28.7 MB, 23.0 MB, 17.2 MB, 11.5 MB, 5.7 MB, 0 — HTTP, Other, Mail, DNS		

Figura MR 9: ntop presenta una información detallada sobre el uso de su red por varios clientes y servidores

La principal desventaja de **ntop** es que no da información instantánea, sino promedios y totales a largo plazo. Esto puede hacer que se vuelva difícil diagnosticar un problema repentino.

Cacti

http://www.cacti.net/

Cacti es un front-end (interfaz de usuario) para RRDtool. Almacena toda la información necesaria para crear gráficas en una base de datos MySQL. El front-end está escrito en PHP. Cacti hace el trabajo de mantener las gráficas, fuentes de datos, y maneja la propia recolección de los datos. Hay soporte para los dispositivos SNMP, y se pueden escribir guiones específicos para sondear casi cualquier evento de la red.

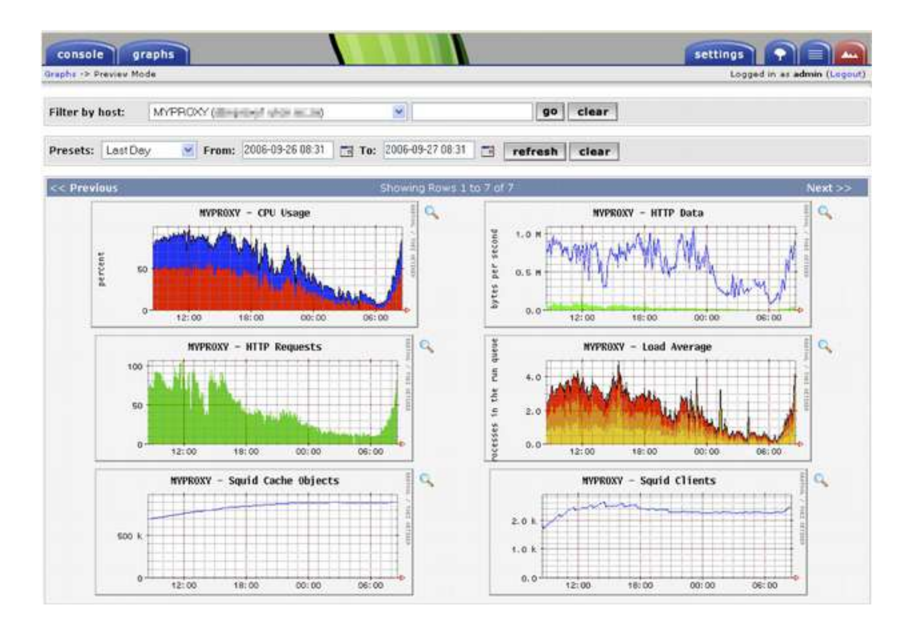


Figura MR 10: Cacti puede manejar el sondeo de sus dispositivos de red. Puede estructurar presentaciones visuales complejas y con mucha información sobre el comportamiento de la red

Cacti puede ser complicado de configurar, pero una vez que entendamos la documentación y los ejemplos puede proporcionar gráficos impresionantes. Hay cientos de plantillas para varios sistemas en el sitio web de cacti, y el código se está actualizando a gran velocidad.

NetFlow

NetFlow es un protocolo inventado por Cisco para colectar información sobre tráfico. En el sitio web de Cisco tenemos esta cita:

NetFlow IOS de Cisco proporciona de manera eficiente un conjunto de servicios clave para aplicaciones IP, incluidos examen de tráfico de la red, facturación basada en el uso, planeamiento de red, seguridad, capacidades de monitoreo de Denegación de Servicio y monitoreo de red. NetFlow ofrece información valiosa sobre los usuarios de la red y aplicaciones, tiempos de uso pico, y enrutamiento de tráfico. Los enrutadores Cisco pueden generar información NetFlow disponible desde el enrutador bajo la forma de paquetes UDP.

NetFlow también hace menos uso de CPU en los enrutadores Cisco que cuando se usa SNMP. También presenta información más atomizada que SNMP, lo que permite tener una visión más detallada del uso de puerto y de protocolo. Esta información se recoge a través de un colector NetFlow que almacena y presenta los datos como un acumulado en el tiempo. Al analizar los datos de flujo se puede armar un cuadro del flujo y el volumen del tráfico en una red o una conexión. Existen varios colectores NetFlow tanto comerciales como gratuitos. Ntop es una herramienta gratuita que puede funcionar como un colector y explorador NetFlow. Al analizar datos de flujo se puede tener una fotografía del flujo y del volumen del tráfico en una red o en una conexión. Hay varias versiones libres o comerciales de estos recolectores Netflow. Ntop es una herramienta gratis que puede funcionar como colector y sonda Netflow. Otra herramienta es Flowc (descrita a continuación). También podría usarse NetFlow como herramienta de monitoreo puntual (*spot check*) al examinar una instantánea de los datos generados en una crisis de red. Considere NetFlow como una alternativa a SNMP para los dispositivos Cisco. Para más información sobre NetFlow: http://en.wikipedia.org/wiki/Netflow.

Flowc

http://netacad.kiev.ua/flowc/

Flowc es un colector NetFlow de fuente abierta (vea NetFlow arriba). Es liviano y de fácil configuración. Usa una base de datos MySQL para almacenar información acumulada de tráfico, lo que permite generar su propio informe a partir de los datos usando SQL, o usar el generador de informes incorporado. Este produce los informes en HTML, sólo texto, o formato gráfico.

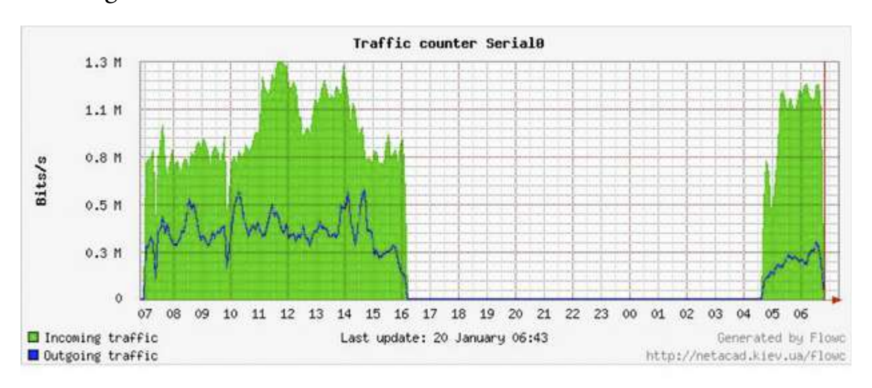


Figura MR 11: Gráfica típica de flujo generada por Flowc

La gran brecha entre los datos probablemente indica un apagón de la red. Las herramientas de predicción normalmente no notifican sobre los apagones sino que únicamente registran su ocurrencia. Para tener notificación del momento en que ocurre un problema de red, debe usarse una herramienta de monitoreo en tiempo real, como Nagios (ver más adelante).

SmokePing

http://oss.oetiker.ch/smokeping/

SmokePing es una herramienta de lujo para medir latencia, escrita en Perl. Puede medir, almacenar, y presentar la latencia, su distribución y la pérdida de paquetes, todo en una sola gráfica.

SmokePing usa RRDtool para almacenamiento de datos, y puede darnos gráficos muy completos que presenten información al minuto sobre el estado de su conexión de red.

Es muy útil ejecutar SmokePing en un anfitrión que tenga buena conectividad a toda su red. A medida que el tiempo pasa, se revelan las tendencias que pueden señalarnos cualquier tipo de problemas de red. En combinación con MRTG o Cacti se puede observar el efecto que tiene la congestión de la red sobre las pérdidas de paquetes y la latencia.

SmokePing puede opcionalmente enviar alertas en presencia de ciertas condiciones, como cuando se observa una gran pérdida de paquetes durante un largo tiempo. Un ejemplo de cómo actúa SmokePing se presenta a continuación en la figura MR 12.

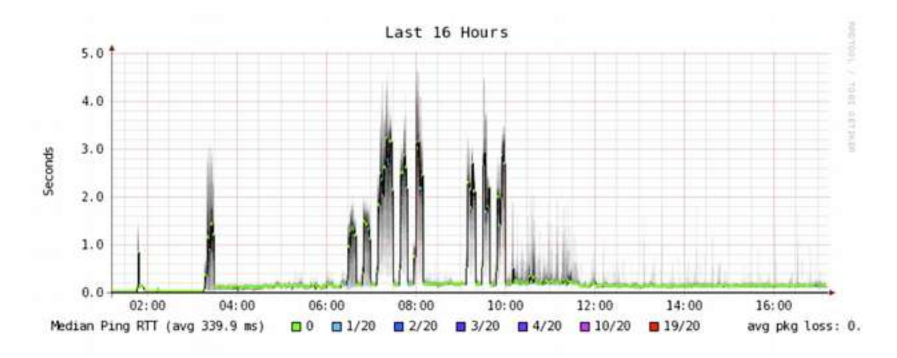


Figura MR 12: SmokePing puede presentar simultáneamente pérdida de paquetes y fluctuaciones de latencia en la misma gráfica

EtherApe

http://etherape.sourceforge.net/

EtherApe proporciona una representación gráfica del tráfico de red. Los anfitriones y los enlaces cambian de tamaño dependiendo del tamaño del tráfico enviado y recibido. Los colores cambian para representar el protocolo más usado. Igual que con wireshark y tcpdump, los datos pueden ser captados "directamente desde el cable" a partir de una conexión de red en tiempo real, o leídos a partir de un archivo de captura tcpdump. EtherApe no muestra tanto detalle como ntop, pero necesita muchos menos recursos.

iptraf

http://iptraf.seul.org/

IPTraf es un monitor de LAN liviano pero poderoso. Tiene una interfaz **ncurses** y se ejecuta desde un *shell* de comando. IPTraf se toma un tiempo para medir el tráfico observado, y luego presenta varias estadísticas, incluidas las conexiones TCP y UDP, información ICPM y OSPF, flujo de tráfico, errores de la suma de comprobación IP, y otros. Es un programa de uso sencillo que usa recursos mínimos de sistema. Aunque no mantiene un histórico de los datos, es útil para ver un informe instantáneo de uso.

IPTraf

Proto/Port	Pkts	Bytes	PktsTo	BytesTo	PktsFrom	BytesFrom
TCP/80	23	12534	10	559	13	11975
UDP/137	22	1716	11	858	11	858
UDP/53	104	14635	61	4591	43	10044
TCP/25	460	78061	247	52772	213	25289
TCP/53	4	240	4	240	0	0
UDP/123	10	760	5	380	5	380
UDP/138	12	2762	6	1381	6	1381

7 entries Elapsed time: 0:00

Protocol data rates (kbits/s): 0.00 in 0.00 out 0.00 total

Up/Down/PgUp/PgDn-scroll window S-sort X-exit

Figura MR 13: Despliegue de estadísticas de tráfico por puerto usando Iptraf

Argus

http://qosient.com/argus/

Argus es el acrónimo de ***Audit Record Generation and Utilization System***. También es el nombre del gigante de los cien ojos de la mitología griega.

De la página web de Argus:

Argus genera información de estadísticas de flujo, como conectividad, capacidad, demanda, pérdida, demora y fluctuación de tiempo (jitter) para cada transacción. Puede usarse para analizar e informar sobre el contenido de archivos de captación de paquetes, o puede funcionar como un monitor continuo examinando los datos de una interfaz en vivo; generando una bitácora (audit log) de toda la actividad de red observada en el flujo de paquetes. Argus puede desplegarse para monitorizar sistemas individuales, o la actividad de una empresa completa. Como monitor continuo, proporciona modelos de manejo "push" y "pull" que permiten estrategias flexibles para la recolección de datos de auditoría de la red. Los clientes de datos Argus permiten una gama de operaciones, tales como clasificación, acumulación, archivo e informe. Argos tiene dos partes: Un colector *master* que lee los paquetes desde un dispositivo de red, y un cliente que conecta con el master y presenta la estadística de uso. Argus funciona en BSD, Linux y la mayor parte de los otros sistemas UNIX.

NeTraMet

http://freshmeat.net/projects/netramet/

NeTraMet es otra herramienta popular de análisis de flujo. Igual que Argus, NeTraMet consta de dos partes: un colector que reúne información estadística por vía de SNMP, y un administrador que especifica cuál flujo debe observarse. Los flujos se especifican utilizando un lenguaje simple de programación que define las direcciones que se usan en cada extremo, y que pueden incluir Ethernet, IP, información de protocolo, u otros identificadores. NeTraMet funciona en DOS y la mayoría de sistemas UNIX, incluidos Linux y BSD.

Prueba del caudal (throughput)

¿Cuán rápido puede funcionar la red?

¿Cuál es la capacidad real utilizable en un enlace específico de la red?

Usted puede obtener una muy buena estimación de su capacidad de rendimiento inundando el enlace con tráfico y midiendo cuánto demora en transferir los datos.



Figura MR 14: Las herramientas como esta de SpeedTest.net son bonitas, pero no siempre le dan una idea precisa sobre el desempeño de su red

Aunque existen páginas web que pueden hacer una "prueba de velocidad" en su navegador (como http://www.dslreports.com/stest o http://speedtest.net/), esas pruebas producen resultados de exactitud decreciente a medida que el usuario se aleja de la fuente de prueba. Aún peor, no le permiten medir la velocidad de un enlace en particular, sino solamente la velocidad de su enlace a Internet.

Le presentamos dos herramientas que le van a permitir realizar una prueba de rendimiento en su propia red.

ttcp

http://ftp.arl.mil/ftp/pub/ttcp/

Actualmente es una parte estándar de la mayoría de los sistemas tipo Unix. **ttcp** es una simple herramienta de prueba de red. Se ejecuta en cualquiera de los lados del enlace que usted quiera probar. El primer nodo actúa en modo receptor, y el otro transmite:

```
node_a$ ttcp -r -s
node_b$ ttcp -t -s node_a
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001 tcp -> node_a
ttcp-t: socket
ttcp-t: connect
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw
```

Después de recolectar los datos en una dirección, debe invertir el rol de transmisión y recepción para probar el enlace en la otra dirección. Puede probar flujos UDP así como TCP, alterar varios parámetros TCP y el tamaño de la memoria intermedia (*buffer*) para probar la red bajo fuertes exigencias. Además, el usuario puede especificar los datos a enviar en la prueba, en lugar de enviar datos generados al azar.

Recuerde que la velocidad de lectura está en kilobytes, no en kilobits. Multiplique el resultado por 8 para encontrar la velocidad en kilobits por segundo. La única desventaja de ttcp es que lleva años sin actualizarse. Pero afortunadamente el código es de dominio público y es gratuito. Igual que ping y tracerout, ttco se encuentra como herramienta estándar en muchos sistemas.

iperf

http://iperf.sourceforge.net/

Al igual que ttcp, iperf es una herramienta de línea de comandos para estimar el caudal de una conexión de red.

Soporta muchas de las mismas características que ttcp, pero utiliza un modelo "cliente" y uno "servidor" en lugar del par "receptor" y "transmisor".

Para ejecutar iperf, inicie un servidor en un lado y un cliente en el otro:

```
node_a$ iperf -s
node_b$ iperf -c node_a
------------------------------------------------------------
Client connecting to node_a, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[ 5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001
[ ID] Interval      Transfer          Bandwidth
[ 5] 0.0-11.3 sec 768 KBytes        558 Kbits/sec
```

El lado del servidor continuará escuchando y aceptando conexiones del cliente en el puerto 5001 hasta que usted presione control-C para detenerlo. Esto puede ser útil si ejecutamos varias tandas de pruebas desde diferentes lugares. La mayor diferencia entre ttcp e iperf es que iperf está siendo desarrollado activamente, y tiene muchas características nuevas (incluyendo soporte IPv6). Esto lo hace una buena elección cuando construimos redes nuevas.

bing

fttp:// fgouget.free. fr/bing/index-en.shtml

En lugar de inundar de datos una conexión y ver cuánto tiempo toma completar la transferencia, ***Bing*** trata de calcular el caudal disponible de una conexión punto a punto analizando los tiempos de ida y vuelta de paquetes ICMP de varios tamaños. Aunque no siempre es tan preciso como una verdadera prueba de flujo, puede proporcionar un buen cálculo sin transmitir un gran número de bytes.

Puesto que bing trabaja con solicitudes de eco ICMP estándares, también puede calcular el caudal disponible sin la necesidad de ejecutar un cliente especial en el otro extremo, puede incluso tratar de estimar el caudal de otros enlaces fuera de su red. Ya que usa poco ancho de banda, bing puede darle una idea aproximada del rendimiento de la red sin incurrir en los costos que ocasionaría una prueba de inundación.

Herramientas de tiempo real

Es deseable saber cuándo hay gente tratando de penetrar su red, o cuándo falla alguna de sus partes. Ya que ningún/a administrador/a puede monitorear la red todo el tiempo, hay programas que sí lo hacen y le envían alertas cuando hay eventos notables. A continuación presentamos algunas herramientas de fuente abierta que pueden ser de ayuda en este aspecto.

Snort

Snort (http://www.snort.org/) es un analizador y registrador de paquetes (*packet sniffer and logger*) que puede usarse como un sencillo sistema de detección de intrusos. Realiza registros basados en reglas y puede efectuar análisis de protocolos, búsqueda de contenido y correlación de paquetes.

Puede usarse para detectar una variedad de ataques e intentos, como exploración disimulada de puertos, ataques CGI, sondeos SMB, intentos de identificación (*fingerprinting*) de sistema operativo y muchas otras clases de tráfico anómalo. Snort tiene una capacidad de alertar en tiempo real que le permite notificar al administrador sobre problemas en el momento en que ocurren, por medio de una variedad de métodos.

Instalar y ejecutar Snort no es tarea fácil y, dependiendo del tráfico de su red, va a necesitar una máquina monitora dedicada con considerables de recursos. Afortunadamente, Snort está muy bien documentado, y tiene una comunidad de usuarios muy fuerte.

Implementando un conjunto exhaustivo de reglas Snort, usted puede identificar comportamiento inesperado que, de otra manera, le consumirían misteriosamente el ancho de banda hacia Internet.

Consulte http://snort.org/docs/ para tener una lista extensa de recursos de instalación y configuración.

Apache: mod_security

ModSecurity (http://modsecurity.org) es un motor de fuente abierta para prevención y detección de intrusos para aplicaciones web. Este tipo de herramienta de seguridad también es conocido como ***cortafuego de aplicación web***.

ModSecurity incrementa la seguridad de aplicaciones web contra ataques conocidos y desconocidos. Puede usarse solo, o como un módulo del servidor web Apache (http://www.apache.org/).

Hay una variedad de fuentes para reglas actualizadas mod_security que ayudan a protegerse contra los últimos ataques de seguridad. Un recurso excelente es GotRoot, que mantiene un gran almacén de reglas actualizadas con frecuencia:

http://www.atomicorp.com/wiki/index.php/Atomic_ModSecurity_Rules

La seguridad de las aplicaciones web es importante en la defensa contra los ataques a su servidor web que podrían resultar en el robo de datos personales valiosos, o en el uso del servidor para lanzar ataques o enviar spam a otros usuarios.

Además de ser perjudicial para la red en su totalidad, estas intrusiones pueden reducir considerablemente su ancho de banda.

Nagios

Nagios (http://nagios.org) es un programa de monitoreo de anfitriones y servicios de su red, que le notifica inmediatamente los problemas en el momento en que ocurren. Estos avisos pueden ser por correo, por SMS, o ejecutando un guión, y serán enviados a la persona relevante, o al grupo dependiendo de la naturaleza del problema.

Nagios funciona en Linux o BSD, y proporciona una interfaz web para mostrar la situación de la red hasta el último minuto.

Nagios es extensible, y puede monitorear el estatus de casi cualquier evento en la red. Realiza comprobaciones por medio de la ejecución de guiones pequeños a intervalos regulares y contrasta los resultados comparándolos con una respuesta esperada. Esto puede darnos revisiones más sofisticadas que un simple sondeo de red.

Por ejemplo, ping puede comprobar que una máquina está funcionando, y nmap, informa si un puerto TCP responde a pedidos, pero Nagios puede realmente recuperar una página web, o hacer un pedido de base de datos y verificar que la respuesta no es un error.

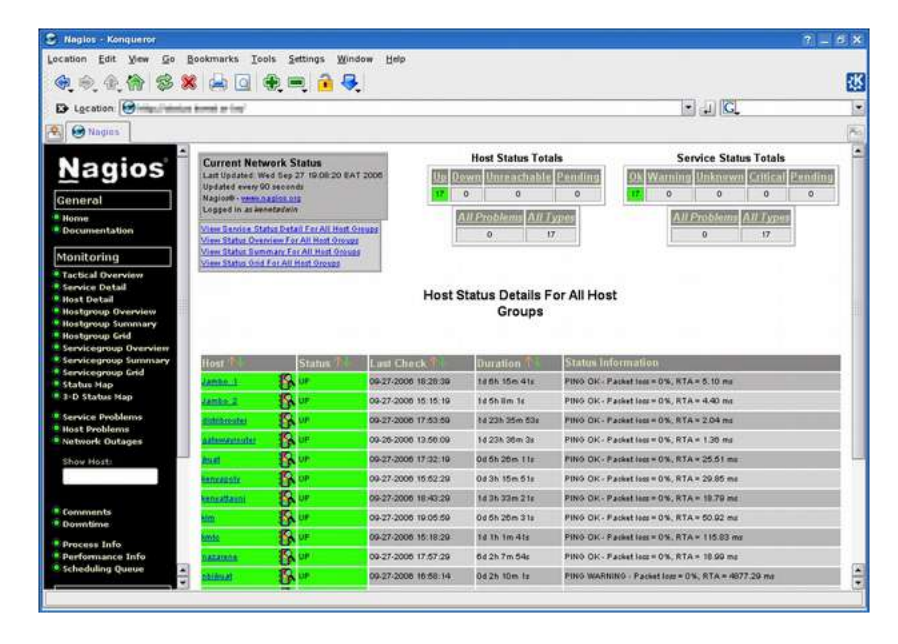


Figura MR 15: Nagios nos mantiene informados sobre el momento en que la red falla, o cuando hay una interrupción de servicio

Nagios puede incluso dejarle saber cuándo el uso de ancho de banda, la pérdida de paquetes, la temperatura del cuarto de máquinas u otros indicadores de la salud de la red, traspasan un determinado umbral.

Esto puede avisarle por adelantado sobre problemas potenciales y a menudo le permite resolverlos antes de que los usuarios se quejen.

Zabbix

Zabbix (http://www.zabbix.org/) es una herramienta de fuente abierta para monitoreo en tiempo real que funciona como un híbrido entre Cacti y Nagios.

Usa una base de datos SQL para almacenamiento, tiene su propio paquete de presentación de gráficos, y realiza todas las funciones que se esperaría de un monitor moderno en tiempo real (como sondeos SNMP y notificación instantánea de condiciones de error). Zabbix está cubierto por la *GNU General Public License.*

Otras herramientas útiles

Hay miles de herramientas de monitoreo de red gratuitas que satisfacen necesidades especiales. Les presentamos algunas de nuestras favoritas que no caen dentro de las categorías anteriores.

[ngrep]

Ngrep proporciona la mayor parte de las características de identificación de patrones del grep de GNU, pero las aplica al tráfico de red. Normalmente reconoce IPv4 e IPv6, TCP, UDP, ICMP, IGMP, PPP, SLIP, FDDI, Token Ring y muchos más.

Puesto que hace uso extenso de la concordancia de expresiones regulares (*regular expression matches*), es una herramienta apropiada para usuarios avanzados o los que tengan buen conocimiento de expresiones regulares.

Pero usted no tiene necesariamente que ser un experto en **regex** para hacer uso básico de ngrep. Por ejemplo, para ver todos los paquetes que contienen la cadena GET (presumiblemente solicitudes HTTP), pruebe lo siguiente:

ngrep -q GET

La concordancia de patrones puede ser restringida aún más para combinarse con ciertos protocolos, puertos u otros criterios, usando filtros BPF. Este es el lenguaje de filtrado usado por las herramientas comunes de análisis de paquetes, como tcpdump y snoop.

Para ver las cadenas de caracteres GET o POST enviadas al puerto de destino 80, use el siguiente comando:

ngrep -q 'GET|POST' port 80

Usando ngrep de manera creativa usted puede detectar desde actividad de virus hasta correo spam. Puede descargarlo en http://ngrepsourceforge.net/.

nmap/Zenmap
nmap es una herramienta de diagnóstico para mostrar el estado y la disponibilidad de los puertos de la red en una interfaz de red. Un uso común es el escaneo de un anfitrión de red en una red TCP/IP para ver cuáles puertos están abiertos y permitiendo de esta manera que se cree un mapa de los servicios de red que proporciona la máquina. La herramienta nmap logra esto mandando paquetes especialmente diseñados a un anfitrión-objetivo y captando la(s) (respuesta(s). Por ejemplo, un servidor web con un puerto 80 abierto pero que no está funcionando responderá de manera diferente a un sondeo nmap que no sólo tiene el puerto abierto sino que está ejecutando httpd.

Asimismo, se obtendrá una respuesta diferente en el caso de un puerto que está simplemente cerrado versus uno que está abierto en un anfitrión pero bloqueado por un cortafuegos.

Con el tiempo, nmap ha evolucionado de ser un simple escáner de puertos a una herramienta que puede detectar versiones del sistema operativo, drivers de la red, el tipo de hardware NIC que usa una interfaz, versiones de los drivers, etc. Además de escanear máquinas individuales, puede escanear redes completas de computadores. Esto significa que nmap podría ser utilizado por usuarios de red maliciosos para "espiar" el sistema antes de atacarlo. Al igual que muchas herramientas de diagnóstico, nmap puede usarse para bien o para mal, y los /las administradores/as deben tener presente estos dos aspectos. La herramienta nmap está bajo la licencia GPL y la última versión se encuentra en http://www.nmap.org.

Zenmap
Zenmap es una multiplataforma GUI que se ejecuta bajo Linux, Windows, Mac OS X, BSD, etc. y puede descargarse también en el sitio nmap.org.

netcat
Entre **nmap** y **tcpdump**, **netcat** es otra herramienta de diagnóstico para investigar puertos y conexiones de la red. Toma el nombre de la utilidad **cat** de UNIX, que simplemente lee cualquier archivo que se le pida. De igual manera, netcat lee y escribe datos a través de cualquier puerto TCP o UDP. La herramienta netcat no es un analizador de paquetes sino que trabaja sobre los datos (payload) contenidos en los paquetes.

Por ejemplo, aquí se muestra cómo correr un servidor web con una sola línea con net cat

{ echo -ne "HTTP/1.0 200 OK\r\n\r\n"; cat some.file; } | nc -l 8080

El archivo some.file será enviado al primer anfitrión que conecte con el puerto 8080 en el sistema que ejecuta netcat.
El comando -1 le ordena a netcat "escuchar" en el puerto 8080 y esperar hasta que logre una conexión.
Una vez lograda, se desbloquea, lee los datos y los manda al clienter conectado al puerto 8080. Otros ejemplos buenos del uso de netcat se encuentran en la entrada netcat de Wikipedia:
https://secure.wikimedia.org/wikipedia/en/wiki/Netcat#Examples
Puede descargar la última versión de netcat en:
http://nc110.sourceforge.net/
Está disponible bajo una Licencia de Software Libre Permisiva.

¿Qué es lo normal?

Si usted está buscando la respuesta definitiva a la pregunta de cómo deberían verse sus patrones de tráfico, va a llevarse una desilusión. No hay respuesta cien por ciento correcta, pero con algún trabajo, podrá determinar lo que es normal en su red. Aunque cada entorno es diferente, algunos de los factores que pueden influir en el aspecto de su tráfico son:

- La capacidad de su conexión a Internet
- El número de usuarios que tienen acceso a la red
- Las políticas sociales (cobro por bytes, cuotas, código de honor, etc.)
- La cantidad, tipos y nivel de los servicios ofrecidos
- La salud de la red (presencia de virus, tráfico de difusión excesivo, lazos de enrutamiento, relevadores de correo abiertos, ataques de denegación de servicios, etc.)
- La competencia de los usuarios de su red
- La ubicación y configuración de las estructuras de control (cortafuegos, servidores proxy, caches, etc.

Esta no es una lista exhaustiva, pero puede darnos una idea de cómo una serie de factores diferentes pueden afectar los patrones de ancho de banda.
Teniendo esto en cuenta, veamos el tema de las pautas de referencia.

Establecer una pauta de referencia (baseline)

Puesto que cada entorno es diferente, usted necesita determinar por sí mismo/a cuál es el aspecto normal de sus patrones de tráfico en condiciones normales. Esto es útil porque le permite identificar los cambios en el tiempo, bien sean repentinos o graduales. Estos cambios, a su vez, pueden ser indicadores de problemas actuales o potenciales en su red.

Por ejemplo, supongamos que su red se detiene y no está seguro/a de la causa. Afortunadamente, usted ha decidido mantener una gráfica de tráfico de difusión como porcentaje del tráfico global de la red. Si esta gráfica muestra un aumento repentino de tráfico de difusión, esto puede interpretarse como que la red ha sido infestada con un virus. Sin la idea apropiada de lo que es "normal" en su red (la pauta de referencia) podría no notar que el tráfico de difusión ha crecido, solo notaría que éste es relativamente alto, lo cual no es necesariamente indicador de problemas. Las gráficas y figuras de la pauta son también muy útiles cuando se quiere analizar los efectos de los cambios introducidos en la red. A menudo es conveniente experimentar con estos cambios probando diferentes valores. Saber cuál es el aspecto de su pauta le va a permitir apreciar si los cambios han mejorado o empeorado las cosas.

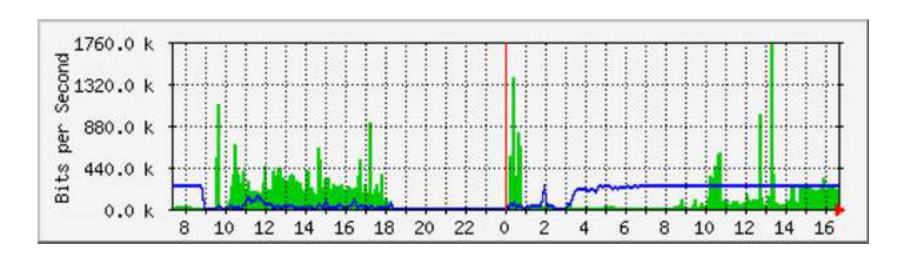


Figura MR 16: Al recoger datos por un período largo, usted podrá predecir le crecimiento de la red y resolver los problemas antes de que se presenten

En la figura anterior podemos observar el efecto que ha tenido sobre la red la implementación de "*delay pools*", alrededor del mes de mayo.

Si no hubiéramos tenido una gráfica de la utilización de la línea, no hubiéramos sabido nunca cuál fue el efecto de este cambio en un período largo de tiempo.

Cuando observamos una gráfica total de tráfico después de haber hecho

cambios, no debe suponerse que se ha perdido el tiempo porque la gráfica no muestra cambios radicales. Usted podría haber sustituido un uso frívolo de su línea por tráfico legítimo. Usted puede combinar esta pauta con otras, por ejemplo, los 100 sitios más contactados, o el uso promedio de los veinte usuarios más frecuentes para determinar si los hábitos de uso han cambiado. Como veremos, MRTG, RRDtool y Cacti, son herramientas excelentes que podemos utilizar para mantener una pauta.

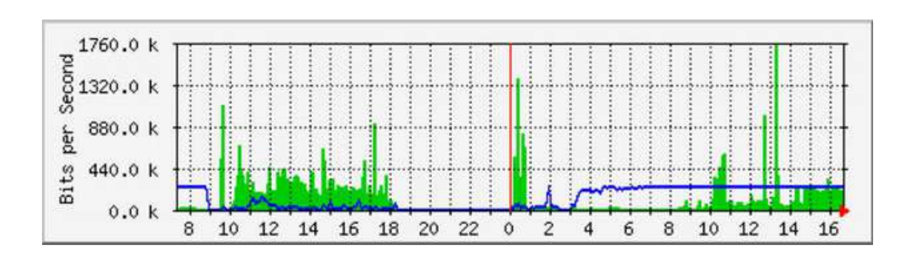


Figura MR 17: La tendencia del tráfico en Aidworld registrada en un solo día

La Figura MR 17 muestra el tráfico en un cortafuego durante un período de 24 horas. Aparentemente no hay nada raro en esta gráfica, pero los usuarios se quejaban de la lentitud de acceso a Internet.

La Figura MR 18 muestra que el uso de ancho de banda de carga (área oscura) era más alto durante las horas laborales del último día que en los días previos. Un período de tráfico de carga fuerte comenzaba cada mañana a las 03:00, y terminaba hacia las 09:00. Pero el último día duró hasta las 16:40. La investigación posterior reveló la presencia de un problema con el software de respaldo que se ejecutaba a las 03:00 cada día.

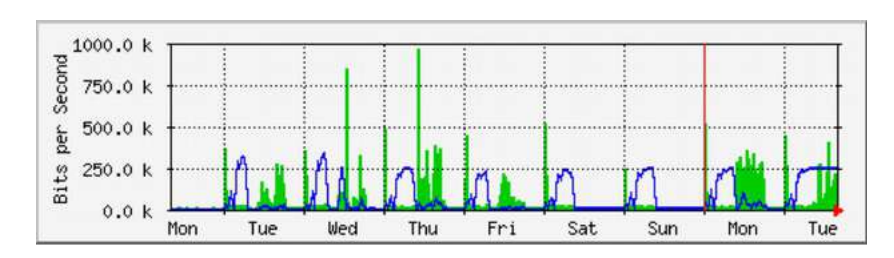


Figura MR 18: La misma red registrada durante una semana entera reveló un problema con los respaldos que causaba una congestión inesperada a los usuarios

La Figura MR 19 muestra los valores de latencia en la misma conexión medidos por el programa SmokePing. La posición de los puntos muestra la latencia promedio mientras que el "humo" gris indica la distribución de la latencia (*jitter*). El color de los puntos indica la cantidad de paquetes perdidos. Esta gráfica de un período de cuatro horas no ayuda a identificar si hay o no problemas en la red.

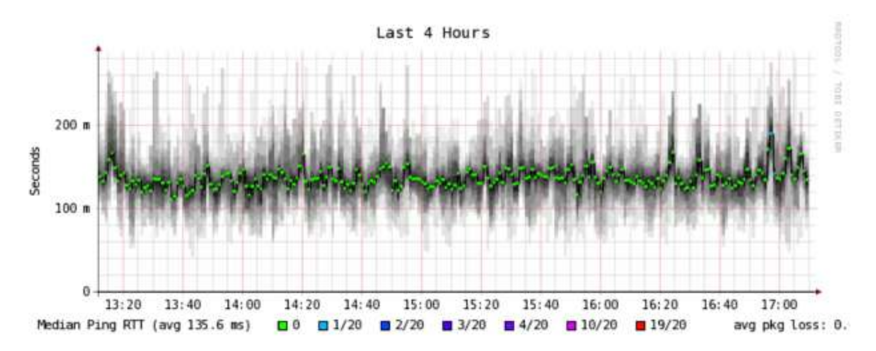


Figura MR 19: Cuatro horas de fluctuación de latencia (jitter) y pérdida de paquetes

La próxima gráfica (Figura MR 20) muestra los mismos datos en un período de 16 horas. Eso indica que los valores de la gráfica superior están cerca de la pauta (*baseline*), pero que hay incrementos considerables de latencia a algunas horas temprano en la mañana, hasta 30 veces por encima de la pauta. Esto indica que debe haber un monitoreo extra de estas horas de la mañana para establecer las causas de la alta latencia, que van a ser probablemente algún tipo de tráfico pesado.

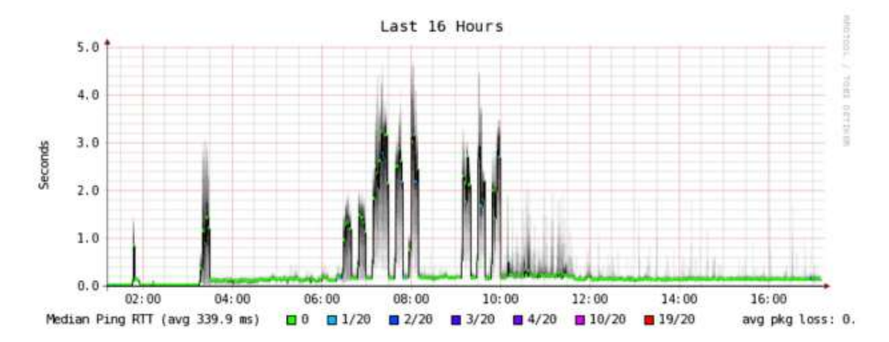


Figura MR 20: Un incremento de la variación de la latencia se muestra en un registro de 16 horas

La Figura MR 21 muestra que el martes fue significativamente peor que el domingo o el lunes respecto a la latencia, especialmente en el período de la mañana temprano. Esto podría indicar que algo ha cambiado en la red.

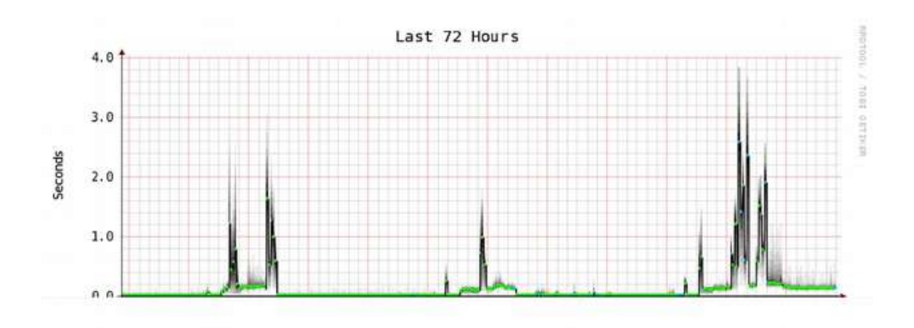


Figura MR 21: Cambiar la escala a una vista semanal revela una repetición definida del aumento de latencia y pérdida de paquetes a primeras horas de la mañana

¿Cómo interpretar las gráficas de tráfico?

En una gráfica básica de flujo de red (como la generada por la herramienta monitor de red MRTG) el área verde indica el tráfico entrante y la línea azul, el saliente.

El tráfico entrante es tráfico que se origina en otra red (normalmente Internet), y va dirigido a un computador dentro de su red. El tráfico saliente se origina en su red y se dirige un computador en algún lugar de Internet.

Dependiendo de qué clase de entorno de red se tenga, la gráfica le va a ayudar a entender cómo está siendo utilizada su red realmente. Por ejemplo, el monitoreo de servidores normalmente revela grandes cantidades de tráfico saliente cuando los servidores responden a las solicitudes (como enviar correos o abrir páginas web), mientras que monitorear las máquinas clientes puede revelar grandes cantidades de tráfico entrante a las máquinas, cuando reciben datos desde los servidores.

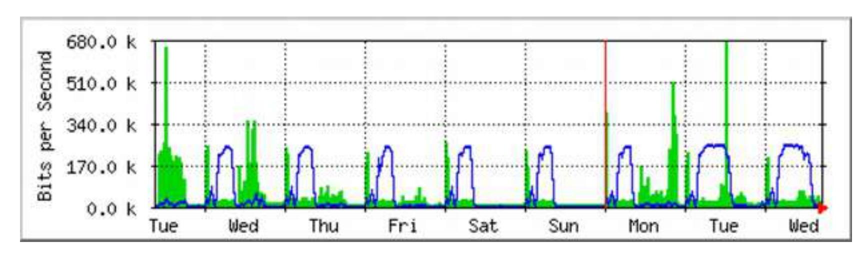


Figura MR 22: Gráfica clásica de flujo de red. El área oscura representa tráfico entrante, mientras que la línea representa el saliente. Los arcos repetidos de tráfico saliente muestran cuándo se ejecutan los respaldos nocturnos

Los patrones de tráfico van a variar dependiendo de lo que use para el monitoreo. Un enrutador va normalmente a mostrar más tráfico entrante que saliente cuando los usuarios descargan datos desde Internet. Un exceso de ancho de banda saliente que no es transmitido por su servidor de red puede indicar un cliente par a par, un servidor no autorizado, o incluso un virus en uno o más clientes. No hay medidas establecidas que indiquen cómo debe aparecer la relación entre tráfico saliente y entrante. Dependerá de usted establecer una pauta para entender cuáles son los patrones de tráfico normales en su red.

Detectando la sobrecarga de la red

La Figura MR 23 muestra el tráfico de una conexión a Internet sobrecargada.

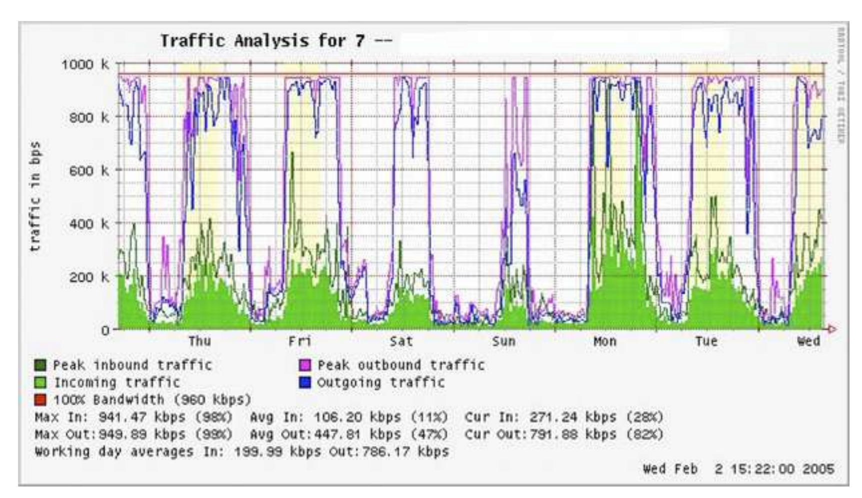


Figura MR 23: Las gráficas de traza plana en el tope indican que una línea está usando el ancho de banda máximo permitido

La señal más obvia de sobrecarga va a ser la línea plana en el tope del tráfico saliente al mediodía cada día.

Las líneas planas pueden indicar sobrecarga incluso si están muy por debajo de la capacidad teórica máxima del enlace. En este caso podría indicar que su proveedor no le está dando el ancho de banda que usted espera.

Para medir el percentil 95

El percentil 95 es un cálculo muy usado en matemáticas para evaluar el uso sostenido y regular de una conexión de red. Su valor muestra el más alto consumo de tráfico en un período determinado.

Calcular el percentil 95 significa que el 95% del tiempo el uso está por debajo de una cierta cantidad, y 5%, por encima de la misma.

El percentil 95 es útil para mostrar el ancho de banda que se usa, al menos el 95% del tiempo.

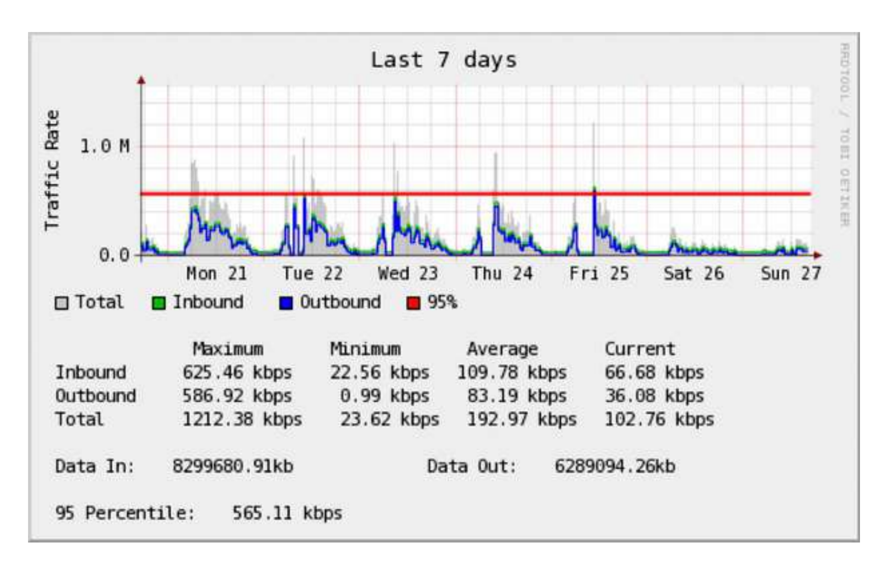


Figura MR 24: La línea horizontal muestra el valor del percentil 95

MRTG y Cacti le van a hacer el cálculo del percentil 95. Esta es una gráfica de muestra de una conexión de 960 kbps. El percentil 95 es de 945 kbps después de descartar el 5% más alto del tráfico.

Monitoreo de RAM y uso del CPU

Por definición, los servidores dan servicios claves que deberían estar siempre disponibles. Los servidores reciben y responden las solicitudes de los clientes prestando servicios que constituyen la razón principal de tener una red. Por lo tanto, deben tener la capacidad de hardware suficiente para realizar la carga de trabajo. Esto significa que deben tener RAM adecuada, almacenamiento, y capacidad de procesamiento para atender todas las solicitudes de los clientes. De otra manera, el servidor se tardará en responder o, en el peor de los casos, va a ser incapaz de responder. Puesto que los recursos de hardware son finitos, es importante mantener un registro de cómo se usan sus recursos de red. Si un servidor central (como un servidor de correos o de proxy) se sobrecarga de solicitudes, los tiempos de acceso se enlentecen. Esto se percibe por parte de los usuarios como un problema de red. Hay varios programas que pueden usarse para el monitoreo de los recursos en un servidor. El método más simple en una máquina Windows es acceder el ***Task Manager*** usando las teclas **Ctrl Alt** + **Del** y luego hacer click en la Performance tab. En un sistema que ejecute Linux o BSD, puede escribir **top** en una ventana terminal. Para mantener registros históricos de este rendimiento, puede usarse MRTG o RRDtool.

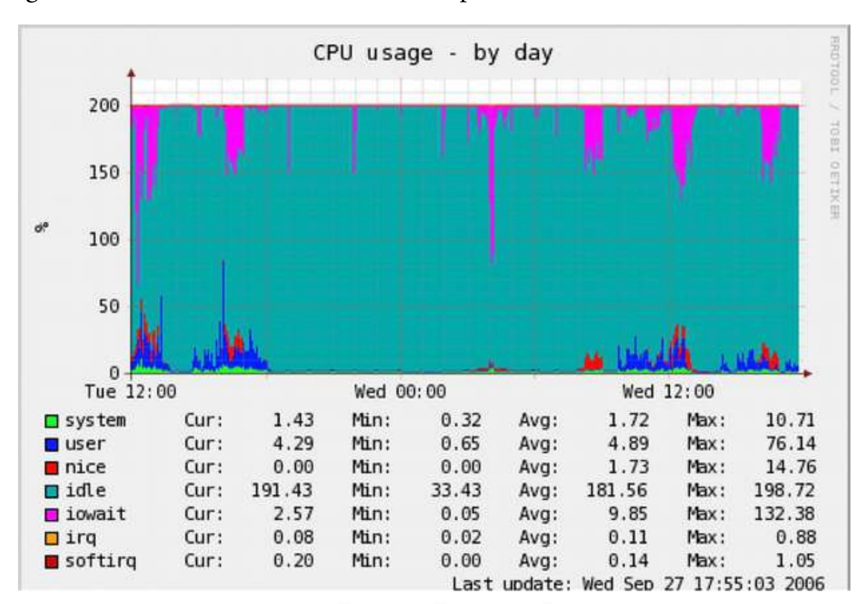


Figura MR 25: RRDtool puede mostrar datos arbitrarios como memoria y uso de CPU, expresados como promedio en el tiempo

Los servidores de correo requieren espacio adecuado, ya que algunas personas prefieren dejar sus mensajes en el servidor por largo tiempo. Los mensajes pueden acumularse y llenar el disco duro, especialmente si hay cuotas sin usar.

Si el disco o la partición usada para almacenar correos se llenan, el servidor no puede recibir correos. Si ese disco es también usado por el sistema van a surgir todo tipo de problemas ya que el sistema operativo se queda sin espacio de intercambio (*swap space*) y de almacenamiento temporal.

El servidor de archivos necesita monitoreo, incluso si tiene discos grandes. Los usuarios van a encontrar la manera de llenar un disco de cualquier tamaño más rápido de lo esperado.

El uso del disco puede ser reglamentado a través del uso de cuotas, o por simple monitoreo y advertencia al usuario de que está haciendo uso excesivo. Nagios puede avisarle cuándo el uso del disco, del CPU u otro recurso del sistema excede los niveles críticos.

Si una máquina deja de responder o se hace lenta, y las mediciones muestran que un recurso está sobre-usado, puede ser una indicación de que se necesita una actualización (*upgrade)*. Si el uso del procesador excede constantemente el 60% del total, probablemente necesite actualizar el procesador. Las velocidades bajas pueden ser indicativas de RAM insuficiente. Asegúrese de comprobar el uso general de la CPU, RAM y espacio de disco antes de tomar la decisión de actualizar un componente en particular.

Una manera sencilla de comprobar si una máquina tiene suficiente RAM es observar la luz del disco duro. Cuando la luz permanece encendida, normalmente indica que la máquina está enviando grandes cantidades de datos hacia y desde el disco. Esto se conoce como ***thrashing*** y es muy malo para el rendimiento. Puede arreglarse averiguando cuál proceso está usando más RAM y abortarlo (kill) o reconfigurarlo. Si eso falla, el sistema necesita más RAM. Debería determinar siempre si es más rentable la actualización de un componente individual, o comprar una máquina nueva. Algunas computadoras son difíciles o imposibles de actualizar, y a menudo resulta más costoso reemplazar componentes individuales que el sistema completo. Como la disponibilidad de repuestos y de sistemas varía mucho en el mundo, asegúrese de ponderar el costo de los repuestos en comparación con el costo del sistema completo, incluidos el transporte y los impuestos, cuando determine el costo de la actualización.

Resumen

Para concluir, en este capítulo hemos hecho una presentación de cómo monitorear su red y otros recursos de computación de manera rentable y eficiente. Le hemos presentado nuestras herramientas preferidas para que sirvan de ayuda, muchas de las cuales han sido probadas por numerosos operadores de red. Esperamos haber explicado la importancia del monitoreo tanto para justificar las actualizaciones necesarias ante los que financian esas actualizaciones, como para atenuar el impacto de los problemas cuando se presentan. Todo esto se traduce en mantener saludable su red y otros recursos de computación y en mantener felices a los usuarios a los que presta el servicio.

17. SOSTENIBILIDAD ECONÓMICA

Introducción

Lograr sostenibilidad a largo plazo es tal vez el objetivo más difícil al diseñar u operar redes inalámbricas en los países en desarrollo. El costo prohibitivo de la conexión a Internet en muchos países, especialmente donde los gobiernos ejercen controles estrictos, impone un gasto operativo sustancial y hace que estos modelos sean sensibles a las fluctuaciones económicas, y que necesiten de cierta innovación para lograr factibilidad.

Desde hace unos pocos años, ha habido un progreso considerable en el uso de redes inalámbricas para comunicaciones rurales debido, en gran parte, a avances tecnológicos.

Se han construido enlaces de larga distancia, los diseños de gran ancho de banda son posibles, y hay disponibles medios seguros de acceso a las redes. En comparación, ha habido pocos éxitos en el desarrollo de modelos comerciales sostenibles para redes inalámbricas, especialmente para áreas rurales.

Basado en las experiencias y observaciones de los autores sobre redes existentes, así como en el conocimiento a partir de los mejores ejemplos empresariales, este capítulo enfocará la propuesta de métodos para implementar redes inalámbricas sostenibles.

En la pasada década ha habido un enorme crecimiento de acceso a Internet en todo el mundo. La mayoría de las ciudades tienen redes inalámbricas o DSL, y conexiones a Internet de fibra óptica, lo que es un cambio substancial. Sin embargo, fuera de las áreas urbanas, el acceso a Internet es todavía un reto formidable.

Hay poca infraestructura cableada más allá de las ciudades importantes. Por lo tanto, la solución inalámbrica es una de las pocas opciones para proporcionar acceso a Internet asequible.

Hay ahora modelos de viabilidad demostrada para acceso rural usando tecnología inalámbrica. Este libro ha sido escrito para aquellos que deseen conectar sus comunidades. Los modelos aquí descritos son a escala menor y usan diseños asequibles.

Nuestra meta es proporcionar ejemplos de cómo las redes inalámbricas pueden diseñarse para difundir acceso sostenible donde los grandes operadores de telecomunicaciones no han instalado todavía sus redes en zonas donde usar modelos tradicionales no sería económicamente factible.

Hay dos errores de concepto muy comunes que deben ser aclarados. En primer lugar, muchos suponen que hay un modelo comercial que va a funcionar para todas las comunidades del mundo, y que la clave del éxito es encontrar esa solución tipo “eureka”.

En la práctica no es así. Cada comunidad, pueblo o aldea son diferentes. No hay modelo prescrito que satisfaga las necesidades de todas las zonas. A pesar de que algunos lugares sean semejantes en términos económicos, las características de un modelo comercial sostenible varían de comunidad en comunidad.

A pesar de que un modelo funcione en un poblado, otro poblado cercano puede no tener las características necesarias para que el mismo modelo sea sostenible. En estas circunstancias, se deben diseñar nuevos modelos, para adaptarlos al contexto de esta comunidad en particular.

Otro error es suponer que sostenibilidad tiene una definición común para todo el mundo. A pesar de que este término generalmente significa que un sistema se construye para permanecer indefinidamente, este capítulo se concentrará más en la discusión sobre las condiciones económicas (financieras y gerenciales), que sobre otros aspectos de la sostenibilidad. También, en lugar de plantear horizontes indefinidos, nos centraremos en un período de 5 años –el período de duración útil esperado para las infraestructuras de TIC y tecnologías inalámbricas.

De esta manera, el término sostenibilidad será usado para englobar un sistema diseñado para permanecer aproximadamente durante cinco años. Como explicamos en otro punto de este libro, las redes inalámbricas en las comunidades locales a menudo estimulan el crecimiento de la conectividad y el uso, y la instalación de fibra se está convirtiendo en realidad.

Un modelo sostenible para su red inalámbrica puede fomentar el crecimiento de otras redes e instalaciones de enlaces de fibra más duraderos de mayor ancho de banda.

Las instalaciones inalámbricas, entonces, coexistirán con las de fibra en su red a medida que crecen en tamaño y alcance.

Cuando se escoge y se implementa el mejor modelo para una red inalámbrica hay algunas claves que pueden ayudarle a conseguir el éxito.

Este capítulo no pretende ser una guía para la gerencia de redes inalámbricas sostenibles.

Antes bien, esta es una guía de "cómo hacer" que quiere presentar un enfoque que lo/la capacite para encontrar el modelo que mejor se adapte a su situación.

Las herramientas y la información que contiene este capítulo ayudarán a la gente que implementa redes inalámbricas en los países en desarrollo a que se formulen las preguntas apropiadas, y a que recojan los datos necesarios para definir los componentes más apropiados a su modelo. Recuerde que determinar el mejor modelo no es un proceso secuencial donde cada paso se lleva hasta su culminación. De hecho, el proceso es continuado e iterativo. Todos sus pasos están conectados íntegramente unos con otros, y a menudo hay que volver sobre ellos varias veces a medida que se progresa.

Establezca una misión para el proyecto

¿Qué quiere usted lograr al crear su red?

Parece una pregunta simple. Sin embargo, muchas redes inalámbricas se instalan sin tener una visión clara de lo que se quiere hacer o se espera lograr en el futuro. El primer paso incluye la conformación de esta visión con el estímulo proveniente de su equipo completo o de su personal.

- ¿Cuál es el propósito de la red inalámbrica?
- ¿A quién va a prestar servicio?
- ¿Qué va a hacer la red para satisfacer las necesidades de la comunidad y para crear beneficios tangibles?
- ¿Cuáles son los principios rectores de la red?

Una buena definición de misión expresa el propósito de su red de una forma significativa y concisa a la vez que formula sus valores y servicios. Y, sobre todo, la misión que establezca proporciona una visión de las aspiraciones de su red inalámbrica.

Es importante que cada miembro del equipo involucrado en la creación de su red inalámbrica se incluya en el proceso de definir la misión, lo que ayuda a crear fortalezas futuras. Esto va a generar respaldo y compromiso, no sólo de parte de su personal, sino de sus clientes, socios, y patrocinadores, lo que va a incidir, a la postre, en el logro de sus objetivos principales. En el dinámico mundo de la tecnología, las necesidades de sus clientes y la mejor manera de satisfacerlas cambia rápidamente; por lo tanto, la definición de su misión es un proceso dinámico. Después de fijar la misión inicial con su equipo, debe investigar para determinar si esta concepción inicial se ajusta a las realidades de su entorno. Con base en un análisis del ambiente externo y de sus capacidades internas, usted debe modificar constantemente su concepto de misión a lo largo del ciclo vital de su red inalámbrica.

Evalúe la demanda de ofertas potenciales

El próximo paso en el establecimiento de su modelo de negocios es averiguar la demanda de la comunidad respecto a los productos de la red y sus servicios.

En primer lugar, identifique en la comunidad los individuos, grupos y organizaciones que tienen necesidad de información y que se beneficiarían de las ofertas de una red inalámbrica.

El grupo de usuarios potenciales comprende una amplia gama de individuos y organizaciones que incluyen, pero no exclusivamente, los siguientes:

- Asociaciones de agricultores y cooperativas
- Grupos de mujeres
- Escuelas y universidades
- Empresarios locales y comerciales
- Clínicas de salud y hospitales
- Grupos religiosos
- Organizaciones no gubernamentales (ONG) locales e internacionales
- Agencias gubernamentales locales y nacionales
- Estaciones de radio
- Organizaciones de la industria turística

Una vez que establezca una lista de todos los potenciales usuarios de la red, debe determinar sus necesidades de acceso a la información y a la comunicación. A menudo, la gente confunde servicios y necesidades.

Un agricultor puede necesitar recabar información sobre precios de mercado y condiciones climatológicas para mejorar la producción de su cosecha y sus ventas. A lo mejor, una manera que tiene de obtener esta información es a través de Internet; sin embargo, también podría recibir esta información por SMS (mensajes de texto) en un teléfono celular, o a través de Voz en Internet (VOIP, en inglés). Es importante diferenciar entre necesidades y servicios porque puede haber varias formas de satisfacer las necesidades del agricultor. Su red inalámbrica debe buscar la mejor manera de satisfacerlas, creando así beneficio al más bajo costo para el usuario.
Cuando se determinan las necesidades para la comunidad, es importante averiguar dónde puede la red proporcionar el mayor beneficio tangible para sus usuarios. Por ejemplo, en el pequeño pueblo de Douentza, Mali, el gerente de un telecentro consideró, a través de discusiones con algunas organizaciones locales, los beneficios potenciales de establecer una red inalámbrica.
Él entrevistó una ONG local que planteó su necesidad de enviar informes mensuales a sus oficinas centrales en Bamako. En ese tiempo, no había acceso a Internet en Douentza, de manera que para enviar un correo electrónico con el informe mensual, la ONG enviaba mensualmente a uno de sus empleados a Mopti, lo que ocasionaba gastos de alojamiento y transporte, además de los adicionales generados por la ausencia al trabajo del empleado durante varios días al mes.
Cuando el gerente del telecentro calculó el total de egresos mensuales de la ONG, pudo demostrar el beneficio de la conexión a Internet por el ahorro de gastos de la organización.
La colaboración de socios clave puede ser también necesaria para asegurar la sostenibilidad de su red inalámbrica. En esta etapa, usted debe establecer contacto con socios potenciales y explorar los beneficios mutuos de una cooperación.
Se puede evaluar las necesidades en su comunidad estableciendo contacto con sus clientes potenciales y preguntándoles directamente a través de encuestas, grupos de enfoque, entrevistas, o reuniones municipales.
Hacer investigación a través de revisiones de estadísticas pertinentes, reportes industriales, censos, revistas, periódicos, y otras fuentes secundarias de información, también le dará una mejor perspectiva de su entorno local.

El objetivo de esta recolección de datos es obtener una comprensión detallada de las necesidades de información y comunicación de su comunidad de manera que la red creada responda a esas necesidades.
A menudo las redes inalámbricas que no tienen éxito han olvidado este paso clave. Su red entera debería basarse en las necesidades de la comunidad.
Si usted inicia una red inalámbrica en la que la comunidad no encuentra ningún beneficio tangible o cuyos servicios sean muy costosos, va a fracasar a la postre.

Establezca incentivos apropiados

A menudo, hay pocos incentivos económicos para acceso a Internet por parte de aquellos participantes cuyos ingresos son de nivel básico.
Además, comprar un computador, o un teléfono inteligente, aprender a usarlos, y conseguir acceso a Internet cuesta mucho más de lo que se obtiene en retribución.
Recientemente, ha habido algunos desarrollos de aplicaciones que quieren solucionar esta falta de incentivo, como sistemas de información de mercado, estándares de calidad impuestos por países importadores, e intercambio de bienes. El acceso a Internet se vuelve una ventaja obvia en situaciones donde conocer día a día los precios de los productos pueda hacer una diferencia importante en las ganancias. Establecer los incentivos económicos apropiados es central para el éxito de la red. La red debe proporcionar beneficio económico a sus usuarios de manera tal que compense los costos, o ser lo suficientemente módica como para que los costos sean mínimos y asequibles para los usuarios. Es imprescindible que se diseñe una red con aplicaciones económicas viables y con costos que sean menores que el beneficio económico que proporciona.
Además, al crear una estructura de incentivos adecuada, usted debe involucrar a la comunidad en la creación de la red desde los comienzos del proyecto, asegurando así que la iniciativa sea orgánica y no impuesta desde afuera. Para comenzar, usted debería tratar de responderse las preguntas siguientes:

1. ¿Qué valor económico puede generar la red en beneficio de la economía local e individuos?
2. ¿Qué tanto beneficio económico tangible puede generarse?
3. ¿Pueden solventarse los impedimentos actuales para que se produzcan estas compensaciones económicas?

Al responder estas preguntas, la red debe ser capaz de articular claramente las propuestas de beneficio que va a presentar a los usuarios. Por ejemplo: "Usando la red, usted será capaz de superar los márgenes en sus ventas en un 2 %", o, "Internet le va a permitir un ahorro mensual de X cantidad en costos de teléfono y de transporte". Usted debe calcular cómo su red va a mejorar la eficiencia, reducir los costos o incrementar las ganancias de sus clientes.

Por ejemplo, si la red va a proporcionar información de mercado para la industria local de maíz, debería instalarla cerca de donde los agricultores traen la cosecha para la venta a los comerciantes.

Su red, además debería concentrarse en sistemas de información de mercadeo, proveer hojas de precios diarios ($1 cada una), o instalar terminales para vendedores y comerciantes ($2 por hora). Su red también podría proporcionar maneras para que los agricultores puedan leer información sobre nuevas técnicas y nuevos productos. También podría proporcionar conexión inalámbrica a los comerciantes y alquilarles terminales de bajas prestaciones (*thin-client*) para acceso a Internet. Si la clientela fuera pequeña, se podrían reducir los costos limitando el acceso a imágenes y otros servicios que requieran un considerable ancho de banda. De nuevo, conocer el beneficio tangible que su red va a generarles a los comerciantes, va a permitirle calibrar lo que ellos podrán gastar para pagar por sus servicios.

Investigue los marcos regulatorios para sistemas inalámbricos

Los marcos regulatorios para redes inalámbricas también inciden sobre el modelo de negocios que se quiera implementar.

Primero, investigue si cualquier organización tiene el derecho de usar frecuencias de 2.4 GHz sin licencia. En la mayoría de las situaciones la banda de 2.4 GHz es de libre uso en todo el mundo; sin embargo, en algunos países el uso de esta banda está restringido, o la licencia para su uso es muy costosa. Además, aunque en algunos países las redes inalámbricas sean legales, el operador de la red podría necesitar una licencia para usar las frecuencias de 2.4 GHz lo que hace que el uso sea prohibitivo para cualquiera que no sea un Internet Service Provider establecido, con suficiente flujo de caja como para pagar el costo de la licencia.

Estas restricciones dificultan a las pequeñas comunidades el compartir una red inalámbrica con otros posibles socios u organizaciones.
Otros países son más liberales y no tienen tantas restricciones sobre las redes inalámbricas, de manera que la compartición de la conectividad a Internet es una solución viable.
La moraleja es que hay que hacer estas averiguaciones al comienzo para asegurarse de que su red cumpla con las leyes del país y de la comunidad local. Algunos gerentes de proyectos se han visto obligados a desconectar su red inalámbrica simplemente porque, sin saberlo, estaban violando la ley.

También debe averiguar sobre la legalidad de los servicios de Voice over Internet Protocol (VoIP).

En algunos países este servicio está controlado por regulaciones complicadas. Las normas para los servicios de VoIP y de pasarelas VoIP varían mucho, así que por favor, chequee cuál es la normativa de su país respecto a lo que está legalmente permitido. Puede comenzar por consultar: http://en.wikipedia.org/wiki/Voice_over_IP

Analice la competencia

La próxima fase en la evaluación de su comunidad se refiere al análisis de la competencia en redes inalámbricas. La competencia incluye a las organizaciones que ofrezcan productos y servicios semejantes (por ejemplo, otro proveedor de Internet inalámbrica (WISP); organizaciones que son consideradas sustitutos o alternativas a los productos y servicios que usted proporciona (cibercafés, por ejemplo); y organizaciones que se definen como nuevos participantes en el mercado inalámbrico. Una vez que determine cuáles son sus competidores, debería estudiarlos cuidadosamente.

Puede obtener información sobre ellos en Internet, por teléfono, en sus materiales de propaganda y mercadeo, en sondeos a sus clientes, o visitas a sus sitios web. Genere un archivo para cada competidor.
La información sobre la competencia que recolecte puede incluir una lista de servicios (con información sobre precios y calidad), sus clientes-objetivo, técnicas de servicio al cliente, reputación, mercadeo, etc. Asegúrese de recabar toda información que le ayude a determinar cómo posicionar su red en la comunidad.

Es importante evaluar a la competencia por muchas razones.

En primer lugar, le ayuda a determinar el nivel de saturación del mercado. Conocer lo que ya existe le permitirá determinar de qué manera su red puede proporcionar beneficio tangible a la comunidad.

Además, el análisis de la competencia puede estimular ideas innovadoras para sus ofertas de servicio. ¿Hay algo que usted pueda hacer mejor que los competidores para hacer que sus servicios satisfagan mejor las necesidades de la comunidad? Finalmente, al analizar a la competencia desde el punto de vista de los clientes y al entender sus fortalezas y debilidades, puede determinar sus ventajas competitivas en la comunidad. Ventajas competitivas son aquellas que no pueden ser fácilmente copiadas por la competencia.
Por ejemplo, si su red inalámbrica puede ofrecer exclusivamente una conexión a Internet más rápida que la competencia, esto constituye una ventaja competitiva que facilita la captación de clientes.

Determine costos, precios iniciales y recurrentes

Cuando esté planeando instalar y operar su red inalámbrica, debe determinar los recursos necesarios para arrancar el proyecto, y para su mantenimiento y operación.
Los costos de instalación incluyen todo lo que debe comprar para arrancar su red inalámbrica. Estos gastos abarcan desde la inversión inicial que se hace en hardware, instalaciones, y equipamiento para puntos de acceso (AP), conmutadores, cables, UPS, etc., hasta los costos para cubrir el registro legal de su organización.
Los gastos recurrentes son aquellos en los que se incurre para continuar operando su red inalámbrica, incluidos costos de acceso a Internet, teléfono, préstamos, electricidad, salarios, alquiler de locales, mantenimiento y reparación de equipos, y la inversión normal para reemplazar desperfectos o equipos obsoletos.
Cada parte de su equipo va a dañarse en algún momento, o va a quedar obsoleta, y usted debería reservar algún fondo extra para estos propósitos.

Un método muy común y aconsejable de enfrentar esto es el de tomar el precio del artefacto y dividirlo por un tiempo estimado de duración. A este proceso se le llama **depreciación**.

A continuación, un ejemplo.

La duración de un computador promedio es de unos dos a cinco años. Si su costo inicial fue de USD 1.000, y usted considera que remplazará el computador a los cinco años, la depreciación anual va a ser de USD 200. En otras palabras, usted debe adjudicar USD 16,67 mensualmente para, finalmente, reemplazar ese computador. Para hacer que su proyecto sea sostenible, es de fundamental importancia que usted ahorre este dinero para compensar la depreciación del equipo cada mes.

Guarde estos ahorros hasta que finalmente pueda utilizarlos para costear el reemplazo del computador. Algunos países tienen leyes de impuestos que determinan el período de depreciación para los diferentes tipos de artefactos. De cualquier manera, usted debería ser realista en cuanto a la vida útil de todo el equipo en uso y hacer planes cuidadosos para contrarrestar su depreciación. Trate de establecer todos sus costos por anticipado, y haga estimaciones realistas sobre sus gastos. La siguiente tabla le muestra una forma de clasificar y detallar sus costos. La estructuración de los diferentes costos es un buen instrumento que le ayudará a distinguir entre los costos iniciales y los recurrentes. Es importante investigar sus costos iniciales desde el comienzo y hacer estimaciones realistas de sus gastos recurrentes. Es siempre mejor presupuestar los gastos por encima que por debajo. Con cada proyecto inalámbrico hay siempre gastos imprevistos, especialmente durante el primer año de operaciones cuando se está aprendiendo a administrar mejor la red.

Categorías de costos

Costos laborales

- Consultorías y revisiones
- Definición de costos de programación, pruebas, integración, etc.
- Costos de instalación
- Costos de reclutamiento de personal (introductorios y mantenimiento)
- Costos de manejo/salarios para empleados y contratistas; su propio salario
- Mantenimiento de los equipos de los empleados
- Mantenimiento de software
- Seguridad del personal

Costos no laborales

- Adquisición y producción (hardware: PC, equipos satelitales (VSAT) o de radio enlace, software)
- Equipos auxiliares (conmutadores, cables y cableado, generadores, UPS, etc.)
- Seguridad y protección de datos
- Inventario inicial (sillas, mesas, iluminación, alfombras, cortinas)
- Costos de local (nuevas construcciones, modificaciones, aire acondicionado, instalaciones eléctricas y cajas, rejas de seguridad)
- Costos legales como el registro del negocio
- Costos iniciales de licencias (VSAT)
- Gastos iniciales de mercadeo (volantes, calcomanías, pósters, fiesta de inauguración)
- Costos de operación de hardware y sistemas operativos (Acceso a Internet, teléfono, etc.)
- Depreciación de equipos y hardware
- Gastos de licencias
- Suministros e insumos de oficina (por ej. dispositivos de almacenamiento de datos, papel, carpetas, clips, etc.)
- Mantenimiento de seguridad y protección de datos
- Primas de seguros
- Costos de energía y mantenimiento del suministro
- Pago de préstamos y costos de amortización
- Costos de publicidad
- Impuestos locales
- Servicios legales y de contabilidad

Para mejorar sus probabilidades de sostenibilidad, es generalmente mejor mantener la más baja estructura de costos para su red. En otras palabras, mantenga sus gastos lo más bajo posible. Tome tiempo en indagar sobre sus proveedores, en particular su proveedor de servicios de Internet y localice las mejores ofertas en servicio de calidad. Una vez más, asegúrese de que su compra se corresponda con las necesidades de la comunidad. Antes de instalar un VSAT caro, asegúrese de que en su comunidad haya un número suficiente de individuos y organizaciones que estén dispuestos a usarlo.

Dependiendo de la demanda de acceso a la información y capacidad de pago, un método alternativo de conectividad podría ser más apropiado. No tenga miedo de innovar y sea creativo/a cuando establezca la mejor solución.

No se debe mantener los precios bajos a expensas de la calidad. Puesto que los equipos de baja calidad son más susceptibles a los daños, a la larga podría estar gastando más en mantenimiento. Es difícil prever la cantidad de dinero que gastará en mantener su infraestructura de TIC. A medida que ésta sea más grande y compleja, mayor es la cantidad de recursos laborales y financieros que se deben anticipar para su mantenimiento. Muchas veces esta relación no es lineal sino exponencial. Si usted tiene algún problema de calidad con su equipo después de que esté instalado, puede costarle una cantidad considerable de dinero arreglarlo.

Al mismo tiempo, sus ventas disminuirán porque el equipo no está funcionando como debería. Hay un ejemplo interesante de un gran proveedor de servicios inalámbricos de Internet (WISP, en inglés) que tenía más de 3.000 AP operando por un tiempo. Sin embargo, el proveedor nunca pudo alcanzar el punto de equilibrio porque tenía que gastar mucho en el mantenimiento de todos los AP. Además, la compañía subestimó la corta duración de ese tipo de equipos.

El hardware para TIC tiende a volverse más barato y mejor cada día. Tan pronto como la compañía había invertido tiempo y dinero en instalar la versión de los costosos AP 802.11b de primera generación, fue creado el nuevo estándar “g”. Nuevos competidores diseñaron AP mejores y más económicos y ofrecieron acceso más rápido y más barato a Internet. Finalmente, el primer proveedor de Internet inalámbrica se vio forzado a cerrar la compañía, a pesar de haber sido el líder del mercado al comienzo.

Tenga presente el rápido avance y cambio de la tecnología y piense cuándo es el momento de reinvertir en equipos más nuevos y económicos (o mejores) y cómo hacerlo para mantener su infraestructura competitiva y actualizada.

Como se mencionó antes, es muy importante que ahorre lo suficiente para hacerlo cuando sea necesario. Una vez que haya identificado y delineado sus costos, debería determinar cuánto y cómo cobrar por sus servicios.

Este es un proceso que es complicado y toma tiempo realizarlo correctamente.

Las siguientes claves pueden orientarlo/la cuando tome decisiones respecto a precios.

- Calcule los precios que va a cobrar de manera que cubra todos los costos de proporcionar el servicio, incluidos los gastos recurrentes.
- Tome en cuenta los precios de la competencia.
- Evalúe la cantidad que los clientes están dispuestos a pagar por los servicios, y asegúrese de que sus precios sean concordantes.

Es completamente esencial diseñar un plan financiero antes de comenzar. Usted necesita registrar todos los costos tanto iniciales como recurrentes y hacer cálculos para determinar si el proyecto es sostenible.

Asegure el financiamiento

Una vez que determine sus costos iniciales y recurrentes, y creado su plan de financiamiento, usted va a saber cuánto es el financiamiento que necesita para administrar su red inalámbrica. El próximo paso es buscar y garantizar la cantidad de dinero apropiada para arrancar y gestionar su red inalámbrica.

El método más tradicional de recibir financiamiento para redes inalámbricas en los países en desarrollo es a través de subvenciones provenientes de donantes. Un donante es una organización que otorga dinero u otros tipos de donaciones a una organización o consorcio de organizaciones, con el fin de ayudarles a regentar proyectos o apoyar causas.

Como este financiamiento se otorga en forma de donaciones u otros subsidios, no se espera que sean devueltos por las organizaciones que realizan el proyecto inalámbrico, ni por los beneficiarios del proyecto. Estos donantes incluyen grandes organizaciones internacionales como la Organización de las Naciones Unidas (ONU) y algunas de sus agencias especializadas, como el Programa de Desarrollo de las Naciones Unidas (UNDP en inglés) y la Organización Educativa, Científica y Cultural de las Naciones Unidas (UNESCO). También se consideran donantes las agencias gubernamentales especializadas en desarrollo internacional, como la Agencia Estadounidense para el Desarrollo Internacional (USAID, en inglés), el Departamento para Desarrollo Internacional del Reino Unido (DFID, en inglés), y la Agencia Canadiense para el Desarrollo Internacional (CIDA, en inglés).

Organizaciones grandes como la Fundación Gates, la Red de la Fundación Soros y las compañías privadas son otro tipo de donantes. Comúnmente, recibir fondos puede ser o no un proceso competitivo.

El proceso no competitivo es más inusual, así que en este capítulo vamos a concentrarnos en el proceso competitivo de más alto nivel. La mayoría de los donantes tienen procedimientos complicados para la distribución de financiamiento.

Los autores de este libro no estamos tratando de trivializar este sistema de reglas y regulaciones, sino que vamos a tratar de presentar una visión general de este proceso para aquellas comunidades que tratan de implementar redes inalámbricas en los países en desarrollo.

Durante el proceso competitivo de convocatoria, el donante usualmente hace una **convocatoria de propuestas** (**RFP**, en inglés), o una **convocatoria de solicitudes** (**RFA**, en inglés), por medio de las cuales se invita a organizaciones no gubernamentales, compañías privadas y sus socios, a presentar propuestas donde se expongan los planes para llevar a cabo proyectos de acuerdo con los requisitos de los objetivos y lineamientos del donante. En respuesta a estas RFP o RFA, las ONG y otras organizaciones compiten presentando sus solicitudes, que luego son evaluadas por los donantes basándose en criterios específicos. Finalmente, la organización donante selecciona la propuesta más apropiada y que haya recibido la más alta evaluación para subvencionarla.

A menudo, los donantes también otorgan fondos para financiar directamente las operaciones de una organización, pero lo más frecuente es que la asignación se haga en un proceso competitivo de convocatoria. Otra forma de acceder a los fondos necesarios para comenzar y mantener una red inalámbrica es a través de micro-financiamiento o el otorgamiento de préstamos, ahorros u otros servicios financieros básicos para la gente más necesitada.

En 1970, algunas organizaciones pioneras como ACCION Internacional y el Banco Grameen, otorgaron microcréditos, que es una forma de micro-financiamiento que les permite a personas necesitadas, o emprendedores, recibir préstamos de sumas módicas para fundar pequeñas empresas. A pesar de que estos individuos carezcan de los requisitos tradicionales para obtener préstamos, tales como bienes que puedan ofrecer como garantías, empleos secundarios o fijos, los programas de microcréditos han sido muy exitosos en muchos países en desarrollo.

La situación más común en estos casos es la de una persona, o un grupo que realiza una solicitud de préstamo, y un ente financiador, persona u organización, que otorga el préstamo, proporcionando el dinero bajo la condición de que se devuelva con intereses.

El uso de microcréditos para financiar redes inalámbricas plantea una limitación. Comúnmente los microcréditos otorgan sumas muy pequeñas, y como se necesita un capital grande para adquirir el equipo inicial para implementar una red inalámbrica, a menudo el microcrédito no es suficiente.

Sin embargo, ha habido otras aplicaciones exitosas del microcrédito que han proporcionado tecnología y sus beneficios al mundo en desarrollo.

Un ejemplo de esto es la historia de los operadores de teléfono en pequeños poblados. Estos emprendedores usan los microcréditos para comprar teléfonos celulares y crédito telefónico.

Luego alquilan el uso de estos celulares a las personas de la comunidad, cobrando por llamada, y obteniendo así suficiente dinero para pagar sus deudas y obtener ganancias para ellos y sus familias.

Otros mecanismos de financiamiento para instalar redes inalámbricas es conseguir inversores ángel (*angel investors)*. Los inversores ángel son por lo general personas adineradas que proporcionan capital para iniciar negocios a cambio de una tasa alta de retorno de su inversión.

Ya que las empresas en las que invierten estos financistas son empresas nacientes (*start-ups*) y, por lo tanto, de alto riesgo, los inversores ángel suelen tener otras expectativas además de las tasas de retorno, tales como un puesto en las juntas directivas o algún rol en la organización. Algunos prefieren tener participaciones en la compañía, mientras que otros prefieren las acciones que puedan cambiar al valor nominal, garantizando una salida claramente definida para el financista.

Para proteger sus inversiones, los inversores ángel a menudo piden al proyecto que no se tomen ciertas decisiones sin su aprobación. En vista del riesgo alto que se corre en el desarrollo de mercados, a menudo es difícil conseguir inversores ángel para lanzar una red inalámbrica, pero no es imposible. La mejor manera de encontrar financistas potenciales es a través de su red social y de búsquedas en línea.

Evalúe las fortalezas y debilidades de la situación interna

La calidad de una red se mide por la calidad de la gente que la opera. El equipo humano que usted ponga al frente puede hacer la diferencia entre el éxito y el fracaso.

Esta es la razón por la cual debe analizar las calificaciones y destrezas de su equipo, incluyendo empleados y voluntarios, para evaluarlas en relación con las destrezas que se requieren para un proyecto inalámbrico.

En primer lugar, haga una lista de las habilidades que se necesitan para desarrollar exitosamente un proyecto de red inalámbrica. Las capacidades deben incluir tecnología, recursos humanos, contabilidad, mercadeo, ventas, negociación, áreas legales, operaciones, entre otras. Después, identifique los recursos locales con los que cuenta para satisfacer estas necesidades.

Compare las habilidades de su equipo humano con las destrezas que necesita, e identifique las carencias. Una herramienta usada a menudo para ayudar en esta auto-evaluación es un método de análisis de fortalezas, oportunidades, debilidades, y amenazas, llamado FODA y en inglés WOT (*Strengths, Weaknesses, Opportunities and Threats*). Para llevar a cabo el análisis, especifique sus fortalezas y debilidades internas y detalle las oportunidades externas y amenazas en su comunidad. Es importante ser realista y honesto acerca de sus cualidades y de sus carencias. Asegúrese de distinguir entre la posición de su organización al comienzo de este esfuerzo, y la que podría ocupar en el futuro.

Sus fortalezas y debilidades le permiten evaluar sus capacidades internas y entender mejor lo que su organización puede hacer, así como sus límites. Al entender sus fortalezas y debilidades y compararlas con las de la competencia, usted puede establecer ventajas competitivas en el mercado. También puede identificar las áreas donde se puede mejorar. Las oportunidades y riesgos son factores externos, lo que lo/la capacita para analizar las condiciones reales y cómo estas van a afectar su red. El diagrama que presentamos a continuación le ayudará a crear el análisis FODA de su organización.

Asegúrese de responder las preguntas planteadas y enumere sus fortalezas, oportunidades, debilidades y amenazas en los espacios apropiados.

Fortalezas	Debilidades
¿Qué hace usted bien? ¿Cuáles recursos especiales puede usar? ¿Qué perciben los otros sobre su fortaleza?	¿Qué podría mejorar? ¿Dónde tiene menos recursos que los demás? ¿Qué podrían percibir los otros como sus debilidades?
Oportunidades	**Amenazas**
¿Qué buenas oportunidades se le abren? ¿Cuáles de sus tendencias puede aprovechar? ¿Cómo puede transformar fortalezas en oportunidades?	¿Qué tendencias podrían perjudicarle? ¿Qué está haciendo la competencia? ¿Cuáles riesgos se derivan de sus debilidades?

Armando el conjunto

Una vez que usted haya reunido toda la información, ya está listo/a para armar las partes y decidir cuál es el mejor modelo de red inalámbrica para su comunidad. Con base en análisis internos y externos, debe refinar los términos de su misión y de sus ofertas de servicio. Todos los factores que ha investigado en los pasos anteriores entran en juego cuando determine su estrategia global. Es esencial utilizar un modelo que aproveche las oportunidades y las acciones dentro de los límites del entorno local.

Para esto, usted debe, a menudo, encontrar soluciones novedosas para lograr sostenibilidad. Hay que explorar diferentes ejemplos y discutir los componentes de los modelos implementados en ellos, para entender mejor cómo se llega al modelo adecuado.

En la distante jungla del la República Democrática del Congo, hay un hospital rural en un poblado llamado Vanga, en la provincia de Bandundu. Queda tan lejos que los pacientes viajan durante semanas para llegar, a veces en una combinación de viaje a pie y navegación fluvial. Este poblado, fundado por misioneros Baptistas en 1904, ha servido de hospital durante años. A pesar de su lejanía extrema, es renombrado por sus excelentes instalaciones y por tener el apoyo de misioneros de Alemania y Estados Unidos, quienes mantienen la instalación funcionando.

En 2004, un proyecto financiado por USAID estableció un telecentro en este poblado para ayudar a mejorar la educación en esta comunidad tan aislada; esta instalación de Internet era muy usada por el grupo más educado de la comunidad: el personal del hospital.

El centro había sido una bendición para la comunidad al ofrecer acceso al conocimiento mundial, e incluso acceso a consultas con colegas distantes en Suiza, Francia y Canadá. El centro necesitó un financiamiento casi total para su operación y costos, y el subsidio debía finalizar en 2006. A pesar de que el centró proporcionó un gran beneficio tangible a la comunidad, tuvo algunos inconvenientes, principalmente factores técnicos, económicos, y políticos que limitaron su sostenibilidad. Se formó una comisión para estudiar sus opciones para el futuro. Después de revisar la estructura de costos del centro, se determinó que necesitaba rebajar sus costos y buscar nuevas formas de incrementar las ganancias. Los gastos más grandes eran los de electricidad y acceso a Internet; por lo tanto, se necesitaba un modelo creativo para reducir los gastos del telecentro y proporcionar acceso de manera sustentable.

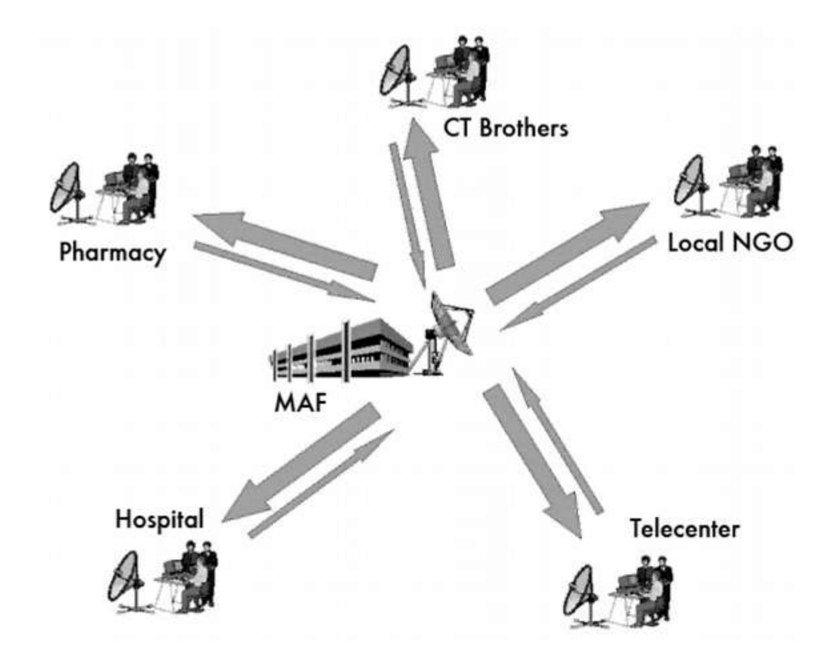


Figura SE 1: Compartiendo Internet con un sistema inalámbrico

En este ejemplo, se usó un VSAT tradicional para dar conectividad. Sin embargo, este modelo proporcionó una forma única de incluir la limitada capacidad de pago de Internet de los grupos locales de la comunidad.

Varias organizaciones en la comunidad compartieron el acceso a Internet por medio de una red inalámbrica; también compartieron los costos asociados con la conexión. Este modelo funcionó bien gracias a condiciones específicas –es decir, la conciencia y la concepción de Internet como un beneficio por parte de miembros clave de la comunidad, los recursos necesarios para proporcionar acceso a Internet, y un sistema regulatorio que permitió compartir el sistema inalámbrico. En Vanga, algunas organizaciones, incluidas el hospital, la farmacia, algunos grupos misioneros, un centro de recursos comunitarios y algunas organizaciones sin fines de lucro tienen la necesidad de acceso a Internet y los medios para pagarlo. Este arreglo hace que la red de organizaciones tenga una conexión de mejor calidad a bajo precio. Adicionalmente, una de las organizaciones del poblado tiene la capacidad y la voluntad de manejar algunos aspectos de la operación de la red, incluyendo emisión y cobro de recibos, mantenimiento técnico y manejo económico general de la red entera. De esta manera, este modelo funciona bien en Vanga porque ha sido diseñado para satisfacer las exigencias de la comunidad y para impulsar los recursos económicos locales.

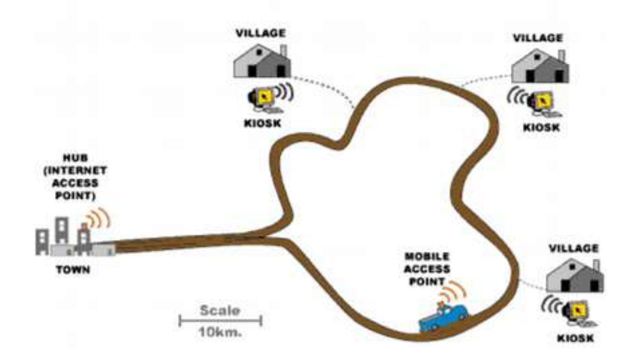


Figura SE 2: Punto de acceso itinerante de DakNet

Otro ejemplo de un modelo adaptado para satisfacer el contexto local es el DakNet de First Mile Solutions. Este modelo ha sido empleado en poblados en India, Cambodia, Rwanda y Paraguay.
Teniendo en cuanta la limitada capacidad adquisitiva de los habitantes, este modelo maneja sus necesidades comunicativas en una forma novedosa.
En el modelo DakNet, hay una franquicia en el país, y se reclutan emprendedores locales para darles entrenamiento en la operación de los kioscos equipados con antenas WiFi.

Por medio de tarjetas pre-pagadas, los habitantes pueden enviar y recibir, —asincrónicamente—, correos electrónicos, textos, y correos de voz, hacer búsquedas en la Web y participar en el comercio electrónico. Estas comunicaciones se almacenan en el servidor local del kiosco. Cuando un autobús o una motocicleta con un punto de acceso itinerante pasa cerca del kiosco, el vehículo en cuestión recibe los datos almacenados y envía los datos recibidos. Una vez que el vehículo llega a un punto con conexión a Internet, procesa todas las solicitudes, transfiere correos electrónicos, mensajes y archivos compartidos. DakNet integra acceso itinerante y modelos de franquicia para proporcionar beneficios tangibles a los habitantes de poblados remotos. Para que este modelo sea sostenible, algunas condiciones clave deben estar presentes. Primero, debe existir una organización de franquicia para proporcionar apoyo financiero e institucional, incluyendo la inversión inicial, capital operativo para ciertos gastos recurrentes, asesoramiento sobre actividades de inicio, entrenamiento de gerencia, procesos estandarizados, mecanismos de reporte y herramientas de mercadeo. Adicionalmente, este modelo necesita una persona del lugar, dinámica y muy motivada que tenga las destrezas apropiadas para manejar un negocio y voluntad de aceptar las sugerencias hechas por la franquicia.
A estos emprendedores se les pide a menudo que empleen su propio capital en los gastos de inicio, de manera que necesitan tener acceso a suficientes recursos económicos. Finalmente, para asegurarse de que este modelo se auto-sostenga, debería haber suficiente demanda de información y comunicación y pocos competidores en la comunidad.

Conclusión

No hay un modelo único para que las redes inalámbricas sean sostenibles en los países en desarrollo; se deben usar y adaptar diferentes modelos de acuerdo con las circunstancias. Cada comunidad tiene características únicas y debe haber suficiente investigación al comienzo del proyecto para determinar el modelo más adecuado. El análisis debe considerar varios factores claves del entorno local, incluyendo demanda en la comunidad, competencia, costos, recursos económicos, etc. A pesar de que una planificación y puesta en marcha adecuadas van a maximizar las posibilidades de que su red sea sostenible, no hay garantías de éxito. Sin embargo, usando los métodos explicados en este capítulo, usted ayudará a garantizar que su red le proporcione a la comunidad beneficios tangibles que se correspondan con sus necesidades.

GLOSARIO

Glosario

0 - 9

802.11. Aunque 802.11 es un protocolo para redes inalámbricas hoy en día obsoleto, 802.11 se usa frecuentemente para referirse a una familia de protocolos utilizados principalmente para redes inalámbricas de área local que incluye 802.11b, 802.11g, y 802.11a. Ver también: ***Wi-Fi***

A

AC: ver Corriente Alterna.

access point (AP). Punto de Acceso. Un dispositivo que crea una red inalámbrica que usualmente está conectado a una red Ethernet cableada. Ver también ***CPE, master mode***

accumulator. Acumulador. Otra denominación para la ***batería***.

ad-hoc mode. Modo ad hoc. Modalidad de los dispositivos 802.11 que permite la creación de una red sin incluir Puntos de Acceso. Las redes en malla frecuentemente operan los radios en la modalidad *ad hoc*. Ver también: ***managed mode, master mode, monitor mode***

Address Resolution Protocol (ARP). Un protocolo muy usado en redes Ethernet para convertir las direcciones IP en direcciones MAC.

address space. Espacio de direcciones. Grupo de direcciones IP que pertenecen a la misma subred lógica.

advertised window. Tamaño de ventana. La porción del encabezamiento TCP que especifica cuántos bytes (octetos) adicionales de datos está dispuesto a aceptar el receptor.

Alternating Current (AC). Corriente Alterna. Corriente que varía en el tiempo, alternándose cíclicamente en valores positivos y negativos. Es la usada normalmente en hogares y oficinas. Ver también ***DC*** (***Direct Current*** –Corriente continua).

amortization. Amortización. Técnica de contabilidad utilizada para tomar en cuenta el costo esperado de reemplazo de los equipos debido a obsolescencia o fin de la vida útil.

amplifier. Amplificador. Dispositivo utilizado para incrementar la potencia de una señal.

amplitude. Amplitud. La distancia desde el centro de una onda al extremo de

uno de sus picos.

Analizador de espectros. Dispositivo que ofrece una representación visual de la potencia de las señales electromagnéticas en función de la frecuencia. Ver también: ***Wi-Spy***.

Ancho de banda. Gama de frecuencias ocupada por una señal. En comunicaciones digitales se usa comúnmente para indicar la ***capacidad*** o tasa de transmisión. Ver también: ***channel, throughput***.

Ancho del haz. Distancia angular entre los puntos a ambos lados del lóbulo principal de una antena en donde la potencia es la mitad de la potencia máxima. Normalmente se expresa para los planos vertical y horizontal.

anchor clients. Clientes Ancla. Clientes corporativos de un sistema de suscripción que son confiables y considerados de bajo riesgo.

AND logic. Lógica AND. Operador lógico cuya salida es verdadera únicamente cuando todas las entradas son también verdaderas. Ver también: ***OR logic (Lógica Or)***.

Anfitrión: Término utilizado para designar cualquier nodo capaz de transmitir y recibir datos en una red.

anonymizing proxy. Proxy Anonimizador. Servicio de red que oculta la fuente y el destino de las comunicaciones, para proteger la privacidad de las personas y para reducir los riesgos legales incurridos por una organización por las acciones de sus usuarios.

anonymity. Anonimato. En redes de computadoras las comunicaciones que no pueden atribuirse a un individuo específico se llaman anónimas. El compromiso entre anonimato y la obligación de rendir cuentas en las comunicaciones en línea es un debate abierto, y las reglas correspondientes a las comunicaciones anónimas varían ampliamente en el mundo. Ver también: ***authenticated (autenticado)***

antenna diversity. Diversidad de antenas. Técnica utilizada para neutralizar la interferencia multitrayectoria mediante el empleo de dos o más antenas físicamente separadas.

antenna gain. Ganancia de Antena. Cantidad en la que se concentra la potencia de una antena en la dirección de su radiación máxima, usualmente expresada en dBi. La ganancia de una antena es recíproca, lo que significa que el incremento de potencia se presenta tanto en transmisión como en recepción.

antenna pattern. Patrón de antena. Gráfico que describe la intensidad relativa del campo radiado por una antena en varias direcciones. Ver también: ***rectangular plot, polar plot, linear polar coordinates, logarithmic polar coordinates***.

AP: ver ***Access Point.***

application layer. Capa de aplicación. La capa superior de los modelos de redes OSI y TCP/IP.

Argus: ver ***Audit Record Generation and Utilization System***.

ARP: ver ***Address Resolution Protocol***.

associated. asociado. Un radio 802.11 se dice asociado a un punto de acceso cuando está listo para comunicarse con la red. Esto significa que está en el canal apropiado, dentro del rango del AP, usa el SSID correcto y otros parámetros de autenticación, etc.

at. Instrucción Unix que permite la ejecución de un programa en un tiempo específico y por una sola vez. Ver también: ***cron***.

attenuation. Atenuación. La reducción de la potencia de una señal a medida que se propaga por su trayectoria, incluyendo la absorción por los árboles, paredes, edificios y otros objetos. Ver también: ***free space loss (pérdida de espacio libre), scattering (dispersión)***.

Audit Record Generation and Utilization System (Argus).

Herramienta de monitoreo de fuente abierta usada para hacer seguimiento de los flujos entre anfitriones (*hosts*). Disponible en *http://www.qosient.com/argus*.

authenticated. Autenticado. Usuario de la red que ha probado su identidad a un servicio o dispositivo (como un punto de acceso) más allá de toda duda, normalmente utilizando criptografía. Ver también: ***anonymity.***

Autoridad de Certificación. Entidad confiable que emite claves criptográficas firmadas. Ver también: ***Public Key Infrastructure, SSL***.

azimuth. Azimut, Acimut. Ángulo que especifica la desviación con respecto al meridiano. Normalmente se mide en sentido de las agujas del reloj desde el norte, pero en astronomía a veces se mide desde el sur. Ver también: ***inclination***.

B

bandwidth. Ancho de banda. Gama de frecuencias ocupada por una señal. En comunicaciones digitales se usa comúnmente para indicar la ***capacidad*** o tasa de transmisión. Ver también: ***channel, throughput***.

battery. Batería. Dispositivo usado para almacenar energía eléctrica, común en sistemas fotovoltaicos. Ver también: ***solar panel, regulator, load, converter, inverter***.

Baterías de plomo-ácido. Baterías constituidas por dos electrodos de plomo sumergidos en un electrolito de ácido sulfúrico diluido en agua. Ver también: ***stationary batteries***.

beamwidth. Ancho del haz. Distancia angular entre los puntos a ambos lados del lóbulo principal de una antena en donde la potencia es la mitad de la potencia máxima. Normalmente se expresa para los planos vertical y horizontal.

benchmarking. Medida de las prestaciones de un servicio o dispositivo. Para medir la tasa de transmisión en una red se la inunda de tráfico y se observa el caudal (*Throughput*) medido tanto en transmisión como en recepción.

BGAN: ver ***Broadband Global Access Network***.

BNC connector. Conector BNC. Conector para cable coaxial que utiliza un mecanismo de bayoneta, utilizado frecuentemente en Ethernet 10base2.

brick. Ladrillo. Término utilizado para referirse a un dispositivo que se ha vuelto inoperable por un error en el proceso de actualización del ***firmware***. También se usa como verbo para indicar la acción de arruinar el dispositivo, que puede ocurrir, por ejemplo, sis e corta la energía durante el proceso de actualización.

bridge. Puente. Dispositivo de red que conecta dos redes a nivel de la ***capa de enlace***. Los puentes no encaminan paquetes en la **capa de red**. Simplemente repiten paquetes entre dos redes locales. Ver también:

router y ***transparent bridging firewall***.

bridge-utils. Un paquete de Linux que se utiliza para crear puentes en redes Ethernet basados en 802.1d. http://bridge.sourceforge.net/

Broadband Global Access Network (BGAN). ***Red de Acceso Global de banda ancha.*** Uno de los varios estándares utilizados para acceso a Internet por satélite. Ver también: ***Digital Video Broadcast (DVB-S)*** y ***Very Small Aperture Terminal (VSAT)***.

broadcast address. Dirección de difusión. En redes IP, la dirección de difusión se usa para enviar datos a todos los anfitriones (***hosts***) en la subred local. En redes Ethernet, la dirección MAC de difusión se utiliza para enviar datos a todas las máquinas en el mismo dominio de colisión.

bypass diodes. Diodos de puenteo. Dispositivos utilizados en algunos paneles solares que evita la formación de ***hot-spots*** (zonas calientes) en las celdas que estén a la sombra, a expensas de la disminución del voltaje total suministrado por el panel.

C

CA: ver ***Certificate Authority***.

Cacti (*http://www.cacti.net/*).

Popular herramienta de monitoreo basada en la web y escrita en PHP.

capacity. Capacidad. La cantidad de tráfico máximo que puede suministrar un sistema de comunicación digital. A menudo incorrectamente llamada ancho de banda.

captive portal. Portal cautivo. Mecanismo utilizado para redireccionar automáticamente los navegadores web hacia un nuevo sitio. A menudo se utilizan para autenticación, o para interrumpir una sesión para, por ejemplo, informar sobre las políticas de usos aceptables.

Caudal. Cantidad real de información por segundo que fluye en una conexión de red, desechando la tara (*overhead*) de los protocolos. A veces se le llama también rendimiento de la transmisión. En inglés *throughput*.

Cell. Celda. Los paneles solares se construyen conectando eléctricamente cierto número de celdas en serie y en paralelo a fin de suministrar un valor especificado de voltaje y corriente. Las baterías también se construyen conectando en serie celdas individuales, cada una de las cuales aporta cerca de 2 voltios a la batería.

Certificate Authority. Autoridad de Certificación. Entidad confiable que emite claves criptográficas firmadas. Ver también: ***Public Key Infrastructure, SSL***.

channel capacity. Capacidad del canal. Cantidad máxima de información que se puede enviar por segundo en un ancho de banda determinado y con una cierta relación señal/ruido. Ver también: ***bandwidth, throughput, data rate***.

channel. Canal. Un rango de frecuencias bien definidas usadas para comunicaciones. En 802.11 cada canal tiene un ancho de banda de 22 MHz, pero la separación de canales es de 5 MHz. Ver también: ***Apéndice B.***

CIDR: ver ***Classless Inter-Domain Routing***.

CIDR notation. Notación CIDR. Método de definir la máscara de red especificando el número de bits presentes. Por ejemplo la máscara 255.255.255.0 puede especificarse como /24 en la notación CIDR.

circular polarization. Polarización circular. Disposición de los campos electromagnéticos, donde el vector de campo eléctrico efectúa una rotación circular perpendicular a la dirección de propagación, describiendo una rotación completa por cada ciclo de la onda. Ver también: ***horizontal polarization, vertical polarization***.

Class A, B, and C networks. Redes Clase A,B y ***C.*** Originalmente el espacio de direcciones IP se adjudicaba en bloques de tres tamaños distintos: Clase A con unos 16 millones de direcciones, clase B con alrededor de 65 mil direcciones y clase C con 255 direcciones. Aunque CIDR ha reemplazado la adjudicación por clases, estas se siguen usando en el interior de organizaciones que usan direcciones privadas, y a menudo se hace referencia a las clases al hablar del espacio de direcciones IP. Ver también: ***CIDR notation***.

Classless Inter-Domain Routing. Enrutamiento entre dominios sin referencia a la clase. CIDR se desarrolló para mejorar la eficiencia del enrutamiento en las dorsales Internet al permitir la agregación de rutas y máscaras de red de tamaño arbitrario. CIDR reemplaza el viejo sistema basado en clases. Ver también: ***Class A, B, and C networks***.

client. Cliente. Un radio 802.11 en modo administrado ***(managed mode).*** Los clientes inalámbricos se conectan a una red creada por un AP y

automáticamente cambiarán su canal para que coincida con el del AP. Ver también: ***access point, mesh.***

closed network. Red cerrada. Aquella en la que el AP no difunde su SSID, utilizado a menudo como una medida de seguridad.

coax. Coaxial. Un cable de sección circular formado por un alambre central rodeado por un dieléctrico, un conductor cilíndrico externo y una cubierta protectora aislante. Los cables de antenas son de este tipo. Coaxial significa con el mismo eje.

collision. Colisión. Las colisiones en una red Ethernet ocurren cuando dos dispositivos conectados al mismo segmento físico intentan transmitir al mismo tiempo. Cuando se detecta una colisión, los dispositivos se abstienen de transmitir por un tiempo breve determinado aleatoriamente.

conductor. Un material que permite el flujo de energía eléctrica o térmica con poca resistencia. Ver también: ***dieléctrico, aislador***.

connectionless protocol. Protocolo sin conexión. Protocolo de red, como por ejemplo UDP, que no requiere el establecimiento o mantenimiento de una conexión. Este tipo de protocolos requiere menos tara (overhead) que los protocolos orientados a conexión, pero no ofrecen protección a los datos o re-ensamblaje de los paquetes. Ver también: ***session oriented protocol***.

consistent platform. Plataforma consistente. Los costos de mantenimiento pueden reducirse al usar una plataforma común con el mismo hardware, software y firmware para muchos componentes de la red.

constructive interference. Interferencia constructiva. Cuando dos ondas de la misma frecuencia se combinan en fase, la amplitud de la onda resultante es la suma de las amplitudes de las dos ondas. A esto se le llama interferencia constructiva. Ver también: ***interferencia destructiva.***

controls. En ***NEC2***, controls define la fuente de RF (radiofrecuencia) en el modelo de la antena. Ver también: ***structure***.

converter. Conversor. Dispositivo utilizado para convertir corriente continua a un voltaje diferente o a corriente alterna. Ver también: ***inverter*** (inversor).

corriente alterna. Corriente que varía en el tiempo, alternándose cíclicamente en valores positivos y negativos. Es la usada normalmente en hogares y oficinas. Ver también: ***DC*** **(*Direct Current –Corriente continua*)**.

CPE: ver ***Customer Premises Equipment***.

cron. Instrucción de Unix que permite la ejecución de un programa a cierta hora incluyendo repeticiones. Ver también: ***at.***

Customer Premises Equipment. Equipo de usuario. Equipo de red tal como un enrutador o un Puente instalado en la propiedad del usuario.

D

data link layer. Capa de enlace. La segunda capa en los modelos de redes OSI o TCP/IP. La comunicación en esta capa ocurre directamente entre nodos. En redes Ethernet se le llama a menudo la capa MAC.

data rate.Tasa de transmisión. La velocidad a la cual los radios 802.11 intercambian símbolos, que es siempre mayor que el caudal (*throughput*) disponible. Por ejemplo, la tasa nominal de 802.11g es 54 Mbps, mientras que el caudal es de unos 20 Mbps. Ver también: ***throughput***.

dB: ver ***decibel***.

DC: ver ***Direct Current***.

DC/AC Converter. Conversor DC/AC. Dispositivo que convierte corriente continua en corriente alterna, requerida por muchos artefactos. También conocido como inversor (***inverter***).

DC/DC Converter. Conversor DC/DC

Dispositivo que cambia el voltaje de una fuente de alimentación contínua. Ver también: ***linear conversion, switching conversion***

decibel (dB). Unidad de medida logarítmica que expresa la magnitud de potencia con respecto a un nivel de referencia. Sus derivadas más comunes son el dBi (decibeles relativos a un radiador isotrópico) y dBm (decibeles relativos a 1 mW).

default gateway. Pasarela por defecto. Cuando un enrutador recibe un paquete destinado a una red para la cual no tiene una ruta específica, lo envía a la pasarela por defecto. La pasarela por defecto repite entonces el proceso, posiblemente enviando el paquete a su propia pasarela por defecto, hasta que el paquete alcanza su destino final.

default route. Ruta por defecto. La ruta que apunta a la pasarela por defecto.

Denial of Service (DoS). Denegación de servicio. Ataque a los recursos de red, usualmente cometido inundando la red de tráfico, o explotando algún error en una aplicación, o en el protocolo de red.

depreciation. Depreciación. Método de contabilidad consistente en apartar dinero para cubrir el costo del eventual reemplazo del equipo.

destructive interference. Interferencia Destructiva. Cuando se combinan dos ondas idénticas que están exactamente en contrafase, la amplitud de la onda resultante es cero. A esto se le llama interferencia destructiva. Ver también: ***constructive interference***.

DHCP: ver ***Dynamic Host Configuration Protocol***.

Dielectric. Dieléctrico. Material no conductor que separa los conductores dentro de un cable.

Digital Elevation Map (DEM). Mapa digital con elevaciones. Datos que representan la altura del terreno para una determinada área geográfica. Estos mapas son usados por programas como ***Radio Mobile*** para modelar la propagación de ondas electromagnéticas.

Digital Video Broadcast (DVB-S). Uno de los varios estándares usado para acceso satelital a Internet. Ver también: ***Broadband Global Access Network (BGAN)*** y ***Very Small Aperture Terminal (VSAT)***.

Diodos de puenteo. Dispositivos utilizados en algunos paneles solares que evita la formación de ***hot-spots*** (zonas calientes) en las celdas que estén a la sombra, a expensas de la disminución del voltaje total suministrado por el panel.

dipole antenna. Antena dipolo. La forma más simple de antena ***omnidireccional***.

Direct Current (DC). Corriente continua. Corriente eléctrica que no cambia de dirección en el tiempo. Se usa normalmente para alimentar dispositivos como puntos de acceso y enrutadores. Ver también: ***Corriente Alterna***.

Direct Sequence Spread Spectrum (DSSS). Espectro Ensanchado por secuencia directa. Método de modulación utilizado en los radios 802.11b

directional antenna. Antena direccional. Antena que radia más energía en una dirección particular. Como ejemplos tenemos las Yagi, parabólicas y de guía-onda. Ver también: ***antena omnidireccional, antena sectorial****.*

directivity. Directividad. Característica de una antena de enfocar la energía transmitida en una dirección particular en transmisión, o de recibir más energía de una cierta dirección en recepción

diversit: ver ***antenna diversity****.*

DNS: ver ***Domain Name Service****.*

DNS caching. Al instalar un servidor *cache* de DNS en su red local, las solicitudes de DNS de toda su red pueden ser almacenadas temporalmente en él, mejorando así los tiempos de respuesta. Esta técnica se llama DNS *caching*.

dnsmasq. Un servidor DNS caching y de DHCP de fuente abierta disponible en *http://thekelleys.org.uk/*

Domain Name Service (DNS). Servicio de nombres de dominio. Protocolo de red ampliamente utilizado que convierte las direcciones IP numéricas en nombres.

dominant mode. Modo Dominante. Disposición de los campos electromagnéticos a la frecuencia mínima que puede ser transmitida por una guía-onda de determinadas dimensiones.

DoS: ver ***Denial of Service****.*

DSSS: ver ***Direct Sequence Spread Spectrum****.*

DVB-S: ver ***Digital Video Broadcast***.

Dynamic Host Configuration Protocol (DHCP). Protocolo utilizado por los anfitriones (*hosts*) para determinar automáticamente su dirección IP.

E

eavesdropper. Persona que intercepta subrepticiamente datos como contraseñas, correos electrónicos o conversaciones en línea.

edge. Borde. Lugar donde la red de una organización se encuentra con la de otra. Los bordes se definen por la ubicación de los enrutadores externos, que a menudo actúan como ***cortafuegos***.

electromagnetic spectrum. Espectro Electromagnético. Rango de las diferentes frecuencias de la energía electromagnética, que incluye ondas de radio, microondas, luz visible y rayos X.

electromagnetic wave. Onda Electromagnética. Onda que se propaga en el espacio sin necesidad de un medio de propagación, compuesta de un campo eléctrico y un campo magnético. Ver también: ***onda mecánica***.

elevation: ver ***inclination***.

end span injectors. Inyector de extremo. Dispositivo para ***Power over Ethernet*** 802.3af que suministra energía eléctrica a través del cable Ethernet. Un *switch* o conmutador Ethernet que suministra energía en cada uno de sus puertos es un ejemplo de inyector de extremo. Ver también: ***mid span injectors***.

end-to-end encryption. Cifrado de extremo a extremo. Una conexión cifrada negociada por ambos extremos de una sesión de comunicación, que provee protección más fuerte que el cifrado en la capa de enlace, recomendado en redes no confiables como la Internet.

EtherApe. Herramienta de visualización de redes de fuente abierta disponible en *http://etherape.sourceforge.net/.*

Ethereal: ver ***Wireshark***.

Extended Service Set Identifier (ESSID). Nombre utilizado para identificar una red 802.11. Ver también: ***closed network***.

external traffic. Tráfico externo.Tráfico que se origina, o está destinado a una dirección IP por fuerade la red interna, como por ejemplo, el tráfico de Internet.

F

firestarter. Herramienta gráfica de configuración de cortafuegos Linux disponible en *http://www.fs-security.com/*.

filter. La tabla por defecto utilizada en el sistema de cortafuegos *netfilter* de Linux, utilizada para determinar el tráfico que debería ser aceptado o negado.

firewall. Cortafuego. Enrutador que acepta o rechaza tráfico con base en algún criterio. Constituye una herramienta básica utilizada para proteger toda la red de tráfico no deseado.

firmware. pequeño programa residente en una memoria de sólo lectura reescribible de algún dispositivo que puede ser actualizado por el usuario.

flashing. acción de reprogramar el firmware de un dispositivo.

flush. Acción de eliminar todas las entradas de una tabla de enrutamiento o una cadena de *netfilter*.

forwarding. reenviar. Cuando los enrutadores reciben paquetes destinados a otro anfitrión u otra red, envían el paquete hacia el enrutador próximo más cercano al destino final. Este proceso se denomina reenvío.

forwarding loops. Lazos de reenvío. Error en la configuración de un enrutador que resulta en el reenvío cíclico de paquetes entre dos o más enrutadores. El colapso de la red se evita gracias al valor del TTL que lleva cada paquete, pero los lazos de reenvío deben ser resueltos para una adecuada operación de la red.

free space loss. Pérdida en el espacio libre. Disminución de la potencia de la señal a consecuencia del esparcimiento sobre una superficie mayor a medida que el frente de onda se propaga en el espacio.

frequency. Frecuencia. Número de ciclos por segundo de una onda. Ver también: ***wavelength, Hertz***.

front-to-back ratio. Relación Adelante/Atrás. El cociente entre la máxima ***directividad*** de una antena y su directividad en la dirección opuesta.

fuente conmutada. Fuente de alimentación de corriente continua (incorrectamente llamada fuente de poder) que usa un componente magnético para almacenar temporalmente la energía y transformarla a otro voltaje. Es mucho más eficiente que las fuentes convencionales que usan un transformador y un rectificador y de menor tamaño.

full duplex. Equipo de comunicaciones capaz de transmitir y recibir simultáneamente (como un teléfono). Ver también: ***half duplex***.

fwbuilder. Herramienta gráfica que le permite la creación de guiones para ***iptables*** en una máquina diferente a su servidor y luego transferirlas al servidor. http://www.fwbuilder.org/.

G

Gain. Ganancia. La capacidad de un dispositivo (tal como una antena o un amplificador) de aumentar la potencia de una señal. Ver también: ***decibel.***

gain transfer. Transferencia de ganancia. Comparación de la ganancia de la antena a medir con la de una antena estándar cuya ganancia es conocida.

Ganancia de Antena. Cantidad en la que se concentra la potencia de una antena en la dirección de su radiación máxima, usualmente expresada en dBi. La ganancia de una antena es recíproca, lo que significa que el incremento de potencia se presenta tanto en transmisión como en recepción.

gasification. Gasificación. Producción de burbujas de oxígeno e hidrógeno que ocurre cuando se le sigue suministrando corriente a una batería cargada.

Generador de señales. Un transmisor que emite continuamente a una frecuencia específica.

globally routable. Enrutable globalmente. Direcciones suministradas por un ISP, o por el RIR (Regional Internet Registry) que son alcanzables desde cualquier punto de la Internet. En IPv4 hay unos cuatro mil millones de direcciones IP posibles, aunque no todas son enrutables globalmente.

H

half duplex. Equipo de comunicación capaz de transmitir o recibir, pero nunca simultáneamente (como los radios de dos vías). Ver también: ***full duplex***.

Heliax. Cable coaxial de alta calidad con un conductor central sólido o tubular y un conductor externo corrugado que le permite flexibilidad. Ver también: ***coax.***

Hertz (Hz). Hercio. Unidad de medida de la frecuencia, correspondiente a ciclos por segundo.

HF (***High-Frequency***). ***Alta frecuencia.*** Ondas de radio con frecuencias comprendidas entre 3 y 30 MHz. Se pueden utilizar para transmitir datos a gran distancia, pero con tasas de transmisión muy bajas.

hop. Salto. Recorrido entre dos enrutadores adyacentes. Un servidor web puede estar a varios saltos de su computador local, y los paquetes pasarán de enrutador a enrutador hasta que alcancen su destino final.

Horas Solares Pico. Promedio de irradianza diaria en un área determinada. Equivale al número de horas que recibirían 1w/m2.

horizontal polarization. Polarización Horizontal. Campo electromagnético en el que el campo eléctrico varía linealmente en el plano horizontal. Ver también: ***circular polarization, vertical polarization.***

host. Anfitrión. Cualquier nodo conectado a la red que puede recibir y enviar paquetes.

hot-spot. En una red inalámbrica, un hot-spot es un sitio que ofrece acceso a Internet mediante ***Wi-Fi***, usualmente a través de un ***portal cautivo.*** En un sistema ***fotovoltaico*** ocurre un hot-spot cuando una celda del panel queda en sombra haciendo que funcione como una carga en lugar de generar potencia.

hub. Concentrador. Dispositivo Ethernet que repite los datos recibidos en todos su puertos.

Huygens principle. Principio de Huygens. Principio que establece que cada punto de un frente de onda se puede considerar que genera un infinito número de frentes de ondas que se propagan en todas direcciones. Este concepto se utiliza para modelar la propagación en presencia de obstáculos.

Hz: ver ***Hertz***.

I

IANA: ver ***Internet Assigned Numbers Authority***.

ICMP: ver ***Internet Control Message Protocol***.

ICP: ver ***Inter-Cache Protocol***.

impedance. Impedancia. Cociente entre el voltaje y la corriente en una línea de transmisión, constituido por una resistencia y una reactancia. La impedancia de carga debe adaptarse a la impedancia de la fuente para máxima transferencia de potencia (normalmente 50 ohmios para sistemas de comunicaciones).

inbound traffic. Tráfico entrante. Paquetes de red originados por fuera de la red local, y dirigidos a un destino dentro de ésta. Ver también: ***outbound traffic***.

inclination. Inclinación. Ángulo con respecto al plano horizontal. Ver también: ***azimuth***.

infrastructure mode: ver ***master mode***.

insulator: ver ***dielectric***.

Inter-Cache Protocol (ICP). Protocolo de altas prestaciones usado para comunicar entre *web caches*.

Internet Assigned Numbers Authority (IANA). La organización que administra partes críticas de la infraestructura de Internet incluyendo la adjudicación de las direcciones IP, los servidores DNS raíz y los números de protocolos de servicio.

Internet Control Message Protocol (ICMP). Protocolo de la capa de red usado para informar a los nodos acerca del estado de la red, parte de la pila de

protocolos de Internet. Ver ***Internet protocol suite***.

Internet layer: ver ***network layer****.*

Internet Protocol (IP). Protocolo IP*.* El protocolo de red de uso más común. IP define los anfitriones y las redes que constituyen la Internet global.

Internet protocol suite (TCP/IP). Grupo de protocolos Internet. Familia de protocolos de comunicación que definen la Internet. Estos incluyen TCP, IP, ICMP, y UDP. También llamada ***TCP/IP protocol suite***, o simplemente ***TCP/IP****.*

Intrusion Detection System (IDS). Sistema de detección de intrusos. Un programa que examina el tráfico en la red buscando patrones o datos sospechosos. Un IDS puede realizar una anotación de bitácora (*log entry*), notificar un administrador de red, o tomar acciones directas en respuesta al tráfico indeseable.

inverter: ver ***DC/AC Converter****.*

IP: ver ***Internet Protocol****.*

iproute2. El paquete de herramientas de enrutamiento avanzado de Linux, usado para conformación de tráfico (*traffic shaping*) y otras técnicas avanzadas. Disponible en http://linux-net.osdl.org/.

iptables. Comando principal utilizado para manipular las reglas del cortafuego *netfilter*.

Irradiance. Irradianza. La potencia total de la radiación solar que incide sobre una determinada superficie en W/m^2.

ISM band. Banda ICM. La banda designada por la UIT (Unión Internacional de telecomunicaciones) para uso Industrial, Científico y Médico, utilizable sin necesidad de licencia previa en la mayoría de los países.

isotropic antenna. Antena Isotrópica. Antena hipotética que distribuye su potencia en todas direcciones con la misma intensidad. No es físicamente realizable, pero se utiliza como referencia.

IV characteristic curve. Curva característica IV. Gráfica que representa la corriente producida en función del voltaje generado en una celda o panel solar iluminado.



knetfilter. Interfaz gráfica para configurar cortafuegos con Linux, disponible en *http://venom.oltrelinux.com/.*

known good. Componente cuya funcionalidad ha sido comprobada y que podemos utilizar para sustituir a otro que sospechamos pueda estar averiado en el proceso de identificación de fallas (*troubleshooting*).

L

lag. Demora. Término utilizado para describir una red donde el tiempo de transmisión de los paquetes, también llamado ***latency*** sea considerable.

Lambda: ***(λ)*** ver ***wavelength (longitud de onda)****.*

LAN: ver ***Local Area Network****.*

latency. Latencia*.* Tiempo que tarda un paquete en atravesar una conexión de red. A menudo se utiliza (incorrectamente) para designar el *Round Trip Time* (RTT), puesto que es mucho más fácil medir este último parámetro en una conexión de de área extendida que la verdadera latencia. Ver también: ***Round Trip Time***.

lead-acid batteries. Baterías de plomo-ácido. Baterías constituidas por dos electrodos de plomo sumergidos en un electrolito de ácido sulfúrico diluido en agua. Ver también: ***stationary batteries****.*

lease time. Cuando se utiliza DHCP, las direcciones IP se asignan por un período limitado, conocido como *lease time*, una vez transcurrido éste, el cliente debe solicitar otra dirección IP del servidor DHCP.

Line of Sight (LOS). Línea de vista. Si una persona desde un punto A logra ver un punto B, se dice que existe línea de vista entre ambos puntos.

linear polar coordinates. Coordenadas polares lineales. Gráfica con círculos graduados concéntricos que representan el valor absoluto de una proyección polar. Estos gráficos se utilizan para representar patrones de radiación de las antenas. Ver también: ***logarithmic polar coordinates***

linear conversion. Conversión lineal. Método de convertir voltajes continuos a un valor inferior disipando el exceso de potencia en forma de calor. Ver también: ***switching conversion****.*

linear polarization. Polarización Lineal. Onda electromagnética en la que el campo eléctrico permanece siempre en el mismo plano. El campo eléctrico puede ser vertical, horizontal, o en un ángulo intermedio. Ver también: ***vertical polarization, horizontal polarization****.*

link budget. Presupuesto de potencia. Análisis de los factores que determinan la potencia que alcanza el receptor en un enlace inalámbrico. Partiendo de la potencia de salida del transmisor, hay que considerar las pérdidas en los cables, ganancia de las antenas y pérdidas en el trayecto. El enlace será viable cuando la energía recibida exceda la energía umbral del receptor en un factor denominado margen del enlace.

link layer encryption. Cifrado en capa de enlace. Conexión cifrada entre dispositivos en la misma red local, comúnmente un AP y un cliente. Ver también: ***end-to-end encryption (cifrado de extremo a extremo)****.*

link-local. Los dispositivos de red que están conectados al mismo segmento físico se comunican entre sí directamente y se dicen que son link-local. Este tipo

de conexiones no puede atravesar un enrutador a menos que utilicen algún tipo de encapsulación como un ***tunnel*** o una ***VPN***.

listen. Escuchar. Los programas que aceptan una conexión en un puerto TCP se dice que escuchan en ese puerto.

load. Carga. Equipo que consume energía. Ver también: ***battery, solar panel, regulator, converter, inverter***

Lóbulos laterales. Ninguna antena puede irradiar solamente en la dirección preferida. Inevitablemente irradia también en otras direcciones. Estos picos más reducidos se denominan lóbulos laterales.

Local Area Network (LAN). Red de area local. Una red (típicamente Ethernet) usada dentro de una organización. La parte de la red detrás del enrutador del ISP es generalmente considerada parte de la LAN. Ver también: ***WAN***.

logarithmic polar coordinates. Coordenadas polares logarítmicas. Gráfico formado por círculos graduados concéntricos, espaciados logarítmicamente, que representan el valor absoluto de una proyección polar. Comúnmente se usan para representar el patrón de radiación de una antena. Ver también: ***linear polar coordinates***.

long fat pipe network. Conexión de red (tal como una VSAT) que tiene gran capacidad y gran latencia. Para obtener buenas prestaciones, TCP debe entonarse para ajustarse a las características de estas redes.

LOS: ver ***Line of Sight***.

M

MAC layer: ver ***data link layer***.

MAC address. Dirección MAC. Número de 48 bits asignado unívocamente a todo dispositivo de red cuando es fabricado. La dirección MAC se utiliza para comunicaciones ***link-local***.

MAC filtering. Filtrado por MAC. Método de control de acceso basado en la dirección MAC de los dispositivos que se comunican.

MAC table. Un conmutador (switch) de red debe mantener una lista de las direcciones MAC usadas en cada uno de los puertos físicos, con el fin de distribuir eficazmente los paquetes. Esta información se mantiene en una tabla llamada MAC table.

maintenance-free lead-acid batteries: ver ***lead-acid batteries***.

Man-In-The-Middle (MITM). Hombre en el medio. Tipo de ataque donde un usuario malicioso intercepta todas las comunicaciones entre el cliente y el servidor, con lo que puede manipular la información.

managed hardware. Hardware administrado. Hardware de red que provee una interfaz de administración, contadores de puertos, SNMP y otras

características interactivas.

managed mode. Modo administrado. Modalidad de los dispositivos 802.11 que permite que el radio de una estación cliente se una a una red creada por un AP (Access Point). Ver también: ***master mode, ad-hoc mode, monitor mode***.

master browser. En redes Windows el master browser es el computador que lleva una lista de todos los computadores, comparticiones e impresoras disponibles en **Network Neighborhood**, o **My Network Places**.

master mode. Modalidad de los dispositivos 802.1 que permite que un radio pueda crear una red tal como lo hace un AP. Ver también: ***managed mode, ad-hoc mode, monitor mode***.

match condition. Condición de selección. En *netfilter*, la *match condition* especifica los criterios que determinan el blanco final de un determinado paquete. Los paquetes se pueden seleccionar en función de la dirección MAC, dirección IP de origen o de destino, número de puerto, contenido de los datos, o cualquier otra propiedad.

Maximum Depth of Discharge (DoDmax). Profundidad máxima de descarga. La cantidad de energía extraída de una batería en un ciclo de descarga, expresada como porcentaje.

Maximum Power Point (Pmax). Punto de potencia máxima. Punto en el que la potencia suministrada por un panel solar alcanza su máximo.

MC-Card. Diminuto conector de microondas utilizado en equipos Lucent / Orinoco/Avaya.

mechanical wave. Onda mecánica. Onda causada cuando algún medio u objeto oscila de manera periódica. Ver también: ***electromagnetic wave***

Media Access Control layer: ver ***data link layer***.

mesh. Malla. Red carente de organización jerárquica, donde cada nodo puede transportar el tráfico de otros nodos. Las buenas implementaciones de redes en malla detectan y resuelven automáticamente los problemas de enrutamiento en forma dinámica.

message types. Tipos de mensajes. El tráfico ICMP utiliza tipos de mensajes en lugar de números de puerto para definir la información enviada. Ver también: ***ICMP***.

method of the worst month. Método del peor mes. Método para dimensionar un sistema fotovoltaico de manera que satisfaga las necesidades de energía del mes en el que la demanda de energía eléctrica es mayor con relación a la oferta de energía solar. Al cumplir con el caso más desfavorable, los demás meses no tendrán problemas.

MHF: ver ***U.FL***.

microfinance. Microfinanzas. Provisión de pequeños préstamos, ahorros y otros servicios financieros básicos a las personas más necesitadas del globo.

mid span injectors. Inyector de línea. Dispositivo ***Power over Ethernet*** insertado entre un conmutador Ethernet y el dispositivo que va a ser alimentado. Ver también: ***end span injectors.***

milliwatts (mW). Milivatios. Unidad de potencia correspondiente a una milésima de vatio.

MITM: ver ***Man-In-The-Middle.***

MMCX. Conector de microondas muy pequeño utilizado en equipos de Senao y Cisco.

monitor mode. Modo Monitor. Modalidad de dispositivos 802.11 en la que el radio escucha pasivamente todo el tráfico en la red. Ver también: ***master mode, managed mode, ad-hoc mode.***

monitor port. Puerto de monitoreo. En un conmutador administrado, se puede definir uno más puertos de monitoreo que recibirán el tráfico de todos los demás puertos. Esto permite conectar un servidor de monitoreo de tráfico para observar y analizar los patrones de tráfico.

Multi Router Traffic Grapher (MRTG). Herramienta de fuente abierta usada para graficación y otras estadísticas, disponible en http://oss.oetiker.ch/mrtg/.

multipath. Multitrayectoria. Característica de propagación en la que la presencia de obstáculos refleja las señales y hace que alcancen al receptor habiendo recorrido diferentes trayectos y por lo tanto con diferentes retardos de propagación.

multipoint-to-multipoint: ver ***mesh.***

mW: ver ***milliwatt.***

My TraceRoute (mtr). Herramienta de diagnóstico usada como alternativa al popular programa ***traceroute***, disponible en http://www.bitwizard.nl/mtr/. Ver también: ***traceroute*** / ***tracert***.

N

N connector. Conector N. Robusto conector de microondas utilizado en componentes para exteriores, como antenas y puntos de acceso (AP).

Nagios (http://nagios.org/). Herramienta de monitoreo de tiempo real que registra en bitácora y notifica al administrador las fallas de servicios y de la red.

NAT: ver ***Network Address Translation.***

nat. La tabla usada en el cortafuego ***netfilter*** de Linux para configurar la conversión de direcciones.

NEC2: ver ***Numerical Electromagnetics Code****.*

NetBIOS. Protocolo de la capa de sesión usado para compartir archivos e impresoras en Windows. Ver también: ***SMB***.

netfilter. Mecanismo de fltrado de paquetes utilizado en las versiones modernas de Linux. Utiliza el comando ***iptables*** para manipular las reglas de filtrado. http://netfilter.org/.

netmask (***network mask***). ***Máscara de red***. Número de 32 bits que divide los 16 millones de direcciones IP disponibles en porciones más pequeñas, denominadas subredes. Todas las redes IP usan las direcciones IP en combinación con las máscaras de red para agrupar lógicamente a los anfitriones y las redes.

NeTraMet. Herramienta de fuente abierta disponible en *freshmeat.net/projects/netramet/.*

network address. Dirección de la red. El número IP inferior de una subred. La dirección de la red es utilizada en las tablas de enrutamiento para especificar el destinatario cuando se envían paquetes a un grupo lógico de direcciones IP.

Network Address Translation (NAT). NAT es una tecnología de red que permite que muchos computadores compartan una misma dirección de red válida (enrutable globalmente). Aunque esto es muy útil para resolver el problema del número limitado de direcciones IP disponibles, crea un desafío técnico para para servicios bidireccionales, como Voz sobre IP.

network detection. Herramienta de diagnóstico que muestra información acerca de las redes inalámbricas, tales como el nombre de la red, canal, y método de cifrado utilizado.

network layer. Capa de red. También llamada la capa Internet. Es la tercera capa tanto del modelo OSI como del modelo TCP/IP de redes. Es la que utiliza el protocolo IP, y donde se efectúa el enrutamiento.

network mask: ver ***netmask****.*

ngrep. Programa de fuente abierta para seguridad de redes que permite encontrar patrones en flujos de datos. Disponible gratuitamente en http://ngrep.sourceforge.net/.

node. Nodo. Cualquier dispositivo capaz de enviar y recibir datos en una red. Los AP, enrutadores, computadores y laptops son ejemplos de nodos.

Nominal Capacity (CN). Capacidad nominal. Cantidad máxima de energía que puede ser extraída de una batería completamente cargada. Se expresa en Amperios-hora (Ah), o vatios-hora (Wh).

Nominal Voltage (VN). voltaje nominal. Voltaje de operación de un sistema fotovoltaico, comúnmente 12 ó 24 voltios.

ntop. Herramienta de monitoreo que suministra muchos detalles acerca de las conexiones y protocolos usados en una red de área local. *http://www.ntop.org/.*

null. Nulo. En el patrón de radiación de una antena, un nulo es una zona en la cual la potencia irradiada efectiva es mínima.

nulling. Anulamiento. Caso especial de la interferencia multitrayectoria donde las señales en la antena receptora se anula por la i***nterferencia destructiva*** causada por las señales reflejadas.

number of days of autonomy (N). Número de días de autonomía. Máximo número de días que puede operar un sistema fotovoltaico sin recibir energía significativa del sol.

Numerical Electromagnetics Code (NEC2). Paquete gratuito para modelar antenas que permite fabricar modelos tridimensionales, y luego analizar la respuesta electromagnética de la antena. *http://www.nec2.org/.*



OFDM: ver ***Orthogonal Frequency Division Multiplexing***.

omnidirectional antenna. Antena Omnidireccional. Tipo de antena que irradia con igual intensidad en todas las direcciones del plano horizontal. Ver también: ***antena direccional, antena sectorial***.

one-arm repeater. Repetidor inalámbrico que utiliza un solo radio, con lo que el caudal se reduce en la retransmisión. Ver también: ***repeater***.

onion routing. Herramienta de privacidad, (tal como ***Tor***) que repetidamente rebota sus conexiones TCP sobre numerosos servidores esparcidos en la Internet, envolviendo la información de enrutamiento en varias capas cifradas.

OR logic. Lógica OR. Operación lógica cuyo resultado es verdadero si cualquiera de las entradas que se comparan es verdadera. Ver también: ***AND logic***.

Orthogonal Frequency Division Multiplexing (OFDM). Técnica de modulación que consiste en descomponer una señal de banda ancha en muchas componentes de banda angosta, cada una de las cuales es modulada en frecuencia por una subportadora. Gracias a la propiedad matemática de ortogonalidad de las subportadoras se minimiza la interferencia entre ellas, lo que resulta en una señal más robusta respecto a la multitrayectoria.

OSI network model. Modelo de red de la OSi. Modelo muy popular de redes de comunicaciones definido por el estándar ISO/IEC 7498-1. El modelo OSI consiste de siete capas independientes, de la física, a la de aplicación. Ver también: ***TCP/IP network model***.

outbound traffic. Tráfico Saliente. Paquetes originados en la red local y dirigidos a un destinatario exterior (usualmente algún lugar de Internet). Ver también: ***inbound traffic***.

overcharge. Sobrecarga. Condición de una batería cuando se le sigue aplicando carga mas allá de la capacidad de la misma. En estas condiciones, el electrolito se descompone produciendo gases y se acorta la duración de la

batería. Los ***reguladores*** permiten una pequeña sobrecarga para que las burbujas así formadas ayuden a mezclar el electrolito, pero luego cortan la corriente para evitar daños en la batería.

overdischarge. Sobredescarga. Descargar una batería mas allá de su ***Maximum Depth of Discharge (Profundidad máxima de descarga)***, lo que resulta en deterioro de la misma.

oversubscribe. Sobresuscripción. Permitir un número de usuarios mayor de los que soporta el ancho de banda disponible.



packet. Paquete. En redes IP, los mensajes enviados entre computadores se fraccionan en pequeños trozos llamados paquetes. Cada paquete contiene la información de procedencia, destinación y otros detalles de enrutamiento que permiten entregarlo a su destino. Los paquetes son re-ensamblados en el extremo remoto mediante TCP (u otro protocolo) antes de ser pasados a la aplicación.

packet filter. Filtro de paquetes. Cortafuegos que funcionan en la capa de Internet inspeccionando las direcciones de procedencia y destino, número de puertos y protocolos. Los paquetes son admitidos o rechazados dependiendo de las reglas de filtrado de paquetes.

partition. Apartado.Técnica usada por concentradores de red para limitar el impacto de nodos que transmiten en exceso. El concentrador aísla temporalmente el nodo defectuoso (lo aparta) del resto de la red y lo reconecta después de algún tiempo. Cuando esto ocurre excesivamente es señal de que hay un cliente que consume demasiado ancho de banda, tal como una aplicación ***peer-to-peer*** o un virus en la red.

Pasarela por defecto. Cuando un enrutador recibe un paquete destinado a una red para la cual no tiene una ruta específica, lo envía a la pasarela por defecto. La pasarela por defecto repite entonces el proceso, posiblemente enviando el paquete a su propia pasarela por defecto, hasta que el paquete alcanza su destino final.

passive POE injector: ver ***Power over Ethernet***.

path loss. Pérdida de trayectoria. Disminución de la potencia de la señal debida a la distancia entre el transmisor y el receptor.

Peak Sun Hours (PSH). Horas Solares Pico. Promedio de irradianza diaria en un área determinada. Equivale al número de horas que recibirían 1w/m2.

Pérdida de retorno. Medida logarítmica expresada en dB del cociente entre la potencia reflejada por la antena o la línea de transmisión y la potencia inyectada a la misma. Ver también: ***impedance***.

photovoltaic generator: ver ***solar panel***.

photovoltaic solar energy. Energía solar fotovoltaica. Uso de paneles solares para producir electricidad. Ver también: ***thermal solar energy***.

photovoltaic system. Sistema fotovoltaico. Sistema que convierte la energía de la radiación solar y la almacena para uso posterior. Un sistema fotovoltaico autónomo no necesita estar conectado a la red de energía eléctrica. Ver también: ***battery, solar panel, regulator, load, converter, inverter***.

physical layer. Capa física. La capa inferior de los modelos de red OSI y TCP/IP. La capa física especifica el medio utilizado para la comunicación, tal como cable de cobre, fibra óptica u ondas de radio.

pigtail. Latiguillo. Cable corto y flexible usado en microondas para convertir un conector no estándar en algo más robusto y común. Sirve también para disminuir el esfuerzo mecánico aplicado al conector del radio.

ping. Herramienta de diagnóstico muy popular que utiliza paquetes ICMP de solicitud de eco y sus respuestas para determinar el tiempo de ida y vuelta a un anfitrión en la red. Cuando se transmite un *ping* entre dos máquinas podemos averiguar en qué parte de la trayectoria se interrumpe el flujo de comunicación.

PKI: ver ***Public Key Infrastructure***.

plomb. Una pieza de metal muy pesada que se entierra en el suelo para mejorar la conductividad de la puesta a tierra.

PoE: ver ***Power over Ethernet***.

point-to-multipoint. Punto a Punto (Pt-Mpt). Topología de red en la que varios nodos se conectan a la misma estación central, llamada estación base o AP (***Access Point***). El ejemplo clásico es el de varios laptops que se conectan a un AP para acceder a Internet. Ver también: ***point-to-point, multipoint-to-multipoint***.

point-to-point. Punto a Punto (Pt-Pt). Red inalámbrica constituida únicamente por dos estaciones, usualmente separadas a una gran distancia.Ver también: ***point-to-multipoint, multipoint-to-multipoint***.

Point-to-Point Protocol (PPP). Protocolo de red usado típicamente en líneas seriales (tales comoconexiones discadas) para proveer conectividad IP.

polar plot. Gráfico polar. Gráfico construido proyectando los puntos sobre un eje que rota (radio) con la intersección de uno o varios círculos concéntricos. Ver también: ***rectangular plot***.

polarization. Polarización. Trayectoria del campo eléctrico de una onda electromagnética en el espacio, o en una antena. Ver también: ***horizontal polarization, vertical polarization, circular polarization***.

polarization mismatch. Desacoplamiento de polarización. Condición en la que la antena transmisora y receptora no usan la misma polarización, resultando en pérdida de señal.

policy. En ***netfilter***, *policy* es la acción tomada por defecto cuando ninguna de las reglas de filtrado son aplicables. Por ejemplo, la *policy* por defecto para cualquier cadena puede ser establecida como ACCEPT o DROP.

port counters. Contadores de puertos. Los conmutadores (switches) y enrutadores administrados proveen estadísticas por cada puerto conectado llamadas *port counters*. Estas estadísticas pueden incluir número de paquetes y de bytes entrantes y salientes, así como errores y retransmisiones.

Portal cautivo. Mecanismo utilizado para redireccionar automáticamente los navegadores web hacia un nuevo sitio. A menudo se utilizan para autenticación, o para interrumpir una sesión para, por ejemplo, informar sobre las políticas de usos aceptables.

power. Potencia. Cantidad de energía por unidad de tiempo.

Power over Ethernet (PoE). Técnica utilizada para suministrar corriente continua a un dispositivo utilizando el cableado Ethernet. Ver también: ***end span injectors, mid span injectors***.

PPP: ver ***Point to Point Protocol***.

presentation layer. Capa de presentación. La sexta capa del modelo de red OSI, que especifica la manera de representar los datos, tal como codificación MIME o compresión de los datos.

Presupuesto de potencia. Análisis de los factores que determinan la potencia que alcanza el receptor en un enlace inalámbrico. Partiendo de la potencia de salida del transmisor, hay que considerar las pérdidas en los cables, ganancia de las antenas y pérdidas en el trayecto. El enlace será viable cuando la energía recibida exceda la energía umbral del receptor en un factor denominado margen del enlace.

private address space. Espacio de direcciones privadas. Conjunto de direcciones IP especificadas en RFC1918. Las direcciones privadas o no enrutables se usan a menudo en una organización en combinación con NAT (Conversión de direcciones). El espacio reservado para direcciones privadas incluye 1 0 . 0 . 0 . 0 / 8 , 172.16.0.0/12, y 192.168.0.0/16. Ver también: ***NAT***.

Privoxy (*http://www.privoxy.org/*). Un *web proxy* que ofrece anonimato mediante el uso de filtros. ***Privoxy*** se usa frecuentemente en conjunción con ***Tor***.

proactive routing. Enrutamiento proactivo. Una implementación de ***mesh (red en malla)*** en la que cada nodo tiene conocimiento de todos los otros nodos en la nube de la malla y también de cuáles nodos pueden utilizarse como pasarelas de tráfico. Cada nodo mantiene una tabla de enrutamiento que abarca la totalidad de la nube de la malla. Ver también: ***reactive routing***.

protocol analyzer. Analizador de protocolos. Programa de diagnóstico usado para observar y desensamblar los paquetes de red. Suministran la máxima cantidad de detalles acerca de paquetes individuales.

protocol stack. Pila de protocolos. Conjunto de protocolos que proveen capas de funcionalidad independientes. Ver también: ***OSI network model y TCP/IP network model***.

Proxy. Programa o dispositivo que realiza una acción en representación de otro. Muy comunes los servidores proxy que almacenan localmente las páginas web mas frecuentadas para disminuir el tráfico del enlace a Internet.

PSH: ver ***Peak Sun Hours***.

Public key cryptography. Cifrado de clave pública. Forma de cifrado utilizada por SSL, SSH y otros programas populares de seguridad. Permite que la información cifrada transite sobre una red no segura sin necesidad de distribuir la clave secreta de cifrado.

Public Key Infrastructure (PKI). Infraestructura de clave pública. Mecanismo de seguridad usado en conjunción con ***public key cryptography*** para prevenir los ataques de tipo ***Man-In-The-Middle***. Ver tambien: ***certificate authority***.

Q

quick blow. Tipo de fusible que se funde inmediatamente cuando la corriente que lo atraviesa supera el valor establecido. Ver también: ***slow blow***.

R

radiation pattern: ver ***antenna pattern.***

radio. Porción del espectro electromagnético en la cual se pueden generar ondas al aplicar corriente alterna a una antena. Dispositivo capaz de emitir y recibir estas ondas.

reactive routing. Enrutamiento reactivo. Tipo de malla (***mesh***) en la que las rutas se calculan únicamente en el momento en que se requiere enviar datos a un nodo específico. Ver también: ***proactive routing***.

realtime monitoring. Monitoreo en tiempo real. Herramienta que permite el monitoreo por largos períodos de tiempo y notifica al administrador en el instante en que se produce algún problema.

reciprocity. Reciprocidad. Propiedad de las antenas de presentar las mismas características en transmisión y en recepción.

recombinant batteries: ver ***lead-acid batteries***.

rectangular plot. Diagrama rectangular. Gráfica donde los puntos se ubican en una grilla simple. Ver también: ***polar plot***.

Regional Internet Registrars (RIR). Los 4 mil millones de posibles direcciones IP son administrados por IANA. El espacio ha sido dividido entre grandes subredes, cuya administración ha sido delegada a alguna de las 5 entidades regionales llamadas ***Registrars***, cada una con autoridad sobre una gran área geográfica. Por ejemplo, en América Latina y el Caribe es LACNIC.

regulator. Regulador. Componente de un sistema fotovoltaico que asegura que la batería trabaje en condiciones adecuadas, evitando la sobrecarga y

sobredescarga que podrían disminuir la vida útil de la batería. Ver también: ***solar panel, battery, load, converter, inverter***.

repeater. Repetidor. Nodo configurado para retransmitir el tráfico que no le está destinado, a menudo utilizado para extender el rango útil de una red.

Request for Comments (RFC). Los RFC son una serie de documentos numerados publicados por la Internet Society que describen las ideas y conceptos de las tecnologías de Internet. No todos los RFC son estándares, pero muchos son aprobados explícitamente por el IETF, o en algún momento se convierten en estándares de facto. Los RFC están disponibles en línea en http://rfc.net/.

return loss. Pérdida de retorno. Medida logarítmica expresada en dB del cociente entre la potencia reflejada por la antena o la línea de transmisión y la potencia inyectada a la misma. Ver también: ***impedance***.

reverse polarity (RP). Polaridad Inversa. Conectores de microondas especiales con el género invertido. Como ejemplo tenemos el popular RP-TNC que usan los Linksys, el RP-SMA y el RP-N.

RF transmission line. Línea de transmisión de radiofrecuencia. El medio (usualmente un cable coaxial, heliax, o una guía de onda) que conecta el radio a la antena.

RIR: ver ***Regional Internet Registrars***.

Round Trip Time (RTT). Tiempo de ida y vuelta. Cantidad de tiempo que le toma a un paquete para que la confirmación de su recepción llegue al transmisor. Frecuentemente confundido con la ***latencia***.

rogue access points. Punto de acceso pirata. Un punto de acceso no autorizado instalado incorrectamente por un usuario autorizado o por una persona maliciosa que pretende recabar datos para dañar la red.

Round Robin Database (RRD). Base de datos que almacena información de manera muy compacta y que no se expande en el tiempo. Este es el formato de datos tanto por la herramienta RDD, como por otras herramientas de monitoreo de redes.

router. Enrutador, ruteador, encaminador. Dispositivo que reenvía paquetes entre diferentes redes. El proceso de reenviar paquetes hacia el próximo salto es llamado enrutamiento, ruteo o encaminamiento.

routing. enrutamiento, ruteo o encaminamiento. Proceso de reenviar paquetes entre diferentes redes. El dispositivo que lo realiza se llama enrutador o ruteador.

routing table.Tabla de enrutamiento. Una lista de redes y direcciones IP mantenida por un enrutador para determinar de qué manera deben reenviarse los paquetes. Si un enrutador recibe un paquete para una red que no aparezca en la tabla de enrutamiento, lo enviará a su pasarela por defecto (***default gatewa***y). Los enrutadores operan en la capa de red. Ver también: ***bridge y default gateway***.

RP: ver ***Reverse Polarity***.

RP-TNC. Versión modificada del popular conector de microondas TNC con el género invertido, utilizado por los equipos fabricados por Linksys.

RRD: ver ***Round Robin Database***.

RRDtool. Conjunto de herramientas que permiten crear y modificar bases de datos RDD así como generar gráficos útiles para presentar los datos. RRDtool se usa para hacerle el seguimiento de datos en el tiempo (tales como ancho de banda, temperatura del cuarto de máquinas o carga promedio del servidor) y pueden desplegar esos datos como un promedio en el tiempo. RRDtool se puede obtener en *http://oss.oetiker.ch/rrdtool/.*

Ruta por defecto. La ruta que apunta a la pasarela por defecto.

rsync (http://rsync.samba.org/). Herramienta de fuente abierta para transferencia incremental de archivos usada para mantener ***mirrors*** (servidores espejo).

RTT: ver ***Round Trip Time***.

S

SACK: ver ***Selective Acknowledgment***.

scattering. Dispersión. Pérdida de señal debida a la presencia de objetos pequeños entre dos nodos. Ver también: ***free space loss, attenuation***.

sectorial antenna. Antena sectorial. Antena que radia principalmente en un área específica. El haz puede ser tan amplio como de 180 grados, o tan estrecho como 60 grados. Ver también: ***directional antenna, omnidirectional antenna***.

Secure Sockets Layer (SSL). Tecnología de cofrado de extremo a extremo incorporada prácticamente en todos los navegadores de red (***web browsers***). SSL usa ***public key cryptography*** y una ***public key infrastructure*** para permitir comunicaciones seguras en la web. Cuando usted ve una página cuyo URL comienza con https, está empleando SSL.

Selective Acknowledgment (SACK). Reconocimiento Selectivo. Mecanismo utilizado para superar las ineficiencias del TCP en redes de alta latencia como las VSAT.

Server Message Block (SMB). Protocolo usado en redes Windows para proporcionar servicios de compartición de archivos. Ver también: ***NetBIOS***.

Service Set ID (SSID): ver ***Extended Service Set Identifier***.

session layer. Capa de sesión. Quinta capa del modelo OSI que maneja las conexiones lógicas entre aplicaciones.

session oriented protocol. Protocolo orientado a sesión. Protocolo orientado a sesión (tal como TCP) que requiere inicialización antes de que se pueda proceder al intercambio de datos, así como algunas tareas de limpieza una vez concluido el intercambio. Los protocolos orientados a sesión normalmente ofrecen corrección de errores y reensamblado de paquetes, a diferencia de los protocolos sin conexión. Ver también: ***connectionless protocol***.

shared medium. Medio Compartido. Una red ***link-local*** donde cada nodo puede ver el tráfico de todos los otros nodos.

Shorewall (*http://shorewall.net/*). Herramienta de configuración usada para establecer cortafuegos ***netfilter*** sin necesidad de aprender la sintaxis de ***iptables***.

sidelobes. Lóbulos laterales. Ninguna antena puede irradiar solamente en la dirección preferida. Inevitablemente irradia también en otras direcciones. Estos picos más reducidos se denominan lóbulos laterales.

signal generator. Generador de señales. Un transmisor que emite continuamente a una frecuencia específica.

Simple Network Management Protocol (SNMP). Protocolo diseñado para facilitar el intercambio de información de gestión entre dispositivos de red. SNMP se usa típicamente para sondear conmutadores de red y enrutadores para recopilar estadísticas de operación.

site-wide web cache. Aunque todos los navegadores modernos proveen una memoria temporal local (*cache*), las organizaciones grandes pueden mejorar la eficiencia instalando un ***site-wide web cache*** tal como ***Squid***, que mantiene una copia de todas las solicitudes hechas desde dentro de la organización para agilizar el procesamiento de ulteriores solicitudes al mismo sitio. Ver también: ***Squid***.

slow blow. Fusible lento. Tipo de fusible que permite el paso de una corriente superior a la nominal por un corto tiempo. Ver también: ***quick blow.***

SMA. Un conector de microonda pequeño de rosca.

SMB: ver ***Server Message Block.***

SmokePing. Herramienta que mide, almacena y despliega la latencia, la distribución de la latencia y las pérdidas de paquetes en el mismo gráfico. Disponible en http://oss.oetiker.ch/smokeping/.

SNMP: ver ***Simple Network Management Protocol***

Snort (*http://www.snort.org/*). Sistema muy popular de detección de intrusiones. Ver también: ***Intrusion Detection System***.

SoC: ver ***State of Charge.***

solar module*:* ver ***solar panel.***

solar panel. El componente de un sistema fotovoltaico que convierte la energía

solar en electricidad. Ver también: ***battery, regulator, load, converter, inverter****.*

solar panel array. Arreglo de paneles solares. Conjunto de paneles solares conectados en serie o en paralelo para proporcionar la energía necesaria a una determinada carga.

solar power charge regulator: ver ***regulator****.*

spectrum: ver ***electromagnetic spectrum****.*

spectrum analyzer. Analizador de espectros. Dispositivo que ofrece una representación visual de la potencia de las señales electromagnéticas en función de la frecuencia. Ver también: ***Wi-Spy****.*

Speed. Velocidad. Término genérico usado para referirse a la rapidez de una conexión de red. Una red de "alta velocidad" debería tener baja latencia y capacidad más que suficiente para transportar el tráfico de sus usuarios. Ver también: ***bandwidth (ancho de banda)***, ***capacity***, y ***latency***.

split horizon DNS. DNS de horizonte dividido. Técnica que consiste en ofrecer diferentes respuestas a las solicitudes de DNS en función de la fuente de la solicitud. Se utiliza para dirigir a los usuarios internos a otro grupo de servidores DNS diferente de los que sirven a los usuarios de Internet.

spoof. Sustituir falsamente un dispositivo, usuario o servicio.

spot check tools. Herramientas de comprobación ocasional. Herramientas de monitoreo que se ejecutan únicamente cuando se necesita diagnosticar un problema. Ejemplos: ***ping*** y ***traceroute***.

Squid. Un ***web proxy cache*** muy popular. Es flexible, robusto, con muchas funcionalidades y puede adaptarse a redes de cualquier tamaño. http://www.squid-cache.org/.

SSID: ver ***Extended Service Set Identifier****.*

SSL: ver ***Secure Sockets Layer****.*

standalone photovoltaic system: ver ***photovoltaic system****.*

State of Charge (SoC). Estado de carga. Cantidad de carga presente en una batería, determinada por el voltaje medido y el tipo de batería.

stateful inspection. Reglas de cortafuego que toman en cuenta el estado asociado con un paquete dado. El estado no es parte del paquete y se transmite sobre la Internet, pero es determinado por el propio cortafuego.Las conexiones nuevas, establecidas y relacionadas pueden ser tomadas en cuenta para filtrar los paquetes. La inspección tomando en cuenta el estado es también llamada a veces *connection tracking* (rastreo de conexiones).

stationary batteries. Baterías estacionarias. Baterías diseñadas para estar en una ubicación fija y en un escenario donde el consumo de potencia es más o menos irregular. Las baterías estacionarias pueden soportar ciclos de descarga muy fuerte, pero no están diseñadas para producir grandes corrientes por

breves periodos de tiempo como las baterías automotrices. Ver también: ***lead-acid batteries***.

structure. En ***NEC2***, una descripción numérica de la ubicación de las diferentes partes de una antena y de cómo están interconectados los alambres. Ver también: ***controls***.

subnet mask: ver ***netmask***.

subnets. Subredes. Un subconjunto de redes IP definido por la máscara de red.

switch. Conmutador. Dispositivo de red que provee una conexión temporal dedicada entre nodos que se comunican. Ver también: ***hub***.

switching conversion. Conversión por conmutación. Método de conversión de voltajes continuos que usa un componente magnético para almacenar temporalmente la energía y transformarla a otro voltaje. Es mucho más eficiente que la conversión lineal.

T

target. En *netfilter*, la acción que se debe tomar cuando un paquete cumple con las condiciones de una regla. Algunos *targets* posibles son: ***ACCEPT***, ***DROP***, ***LOG***, y ***REJECT***.

TCP: ver ***Transmission Control Protocol***.

TCP acknowledgment spoofing. *Técnica utilizada en comunicaciones vía satélite para mejorar el caudal de la transmisión. En lugar de esperar la respuesta del extremo satelital remoto, el enrutador en el extremo cercano envía un ACK cuando el paquete está aún en tránsito.*

TCP window size. Tamaño de la ventana TCP. El parámetro de TCP que define cuántos datos pueden ser transmitidos antes de que un paquete ACK sea enviado por el receptor. Por ejemplo, una ventana de 3000 implica que se transmitirán dos paquetes de 1500 bytes cada uno, después de lo cual el extremo receptor enviará un ACK o pedirá una retransmisión.

TCP/IP: ver ***Internet protocol suite***.

TCP/IP network model. Modelo de redes TCP/IP. Simplificación del modelo de redes OSI que se usa con las redes Internet. El modelo TCP/IP consiste de 5 capas independientes, desde la física hasta la de aplicación. Ver también: ***OSI network model***.

tcpdump. Herramienta popular para capturar y analizar paquetes disponible en *http://www.tcpdump.org/*. Ver también: ***WinDump*** and ***Wireshark***.

Temporal Key Integrity Protocol (TKIP). Protocolo de cifrado utilizado en conjunto con ***WPA*** para mejorar la seguridad de una sesión de comunicaciones.

thermal solar energy. Energía solar térmica. Energia del sol recolectada en forma de calor. Ver también: ***photovoltaic solar energy.***

thrashing. Estado de un computador que ha utilizado toda la memoria RAM disponible y debe usar el disco duro para almacenamiento temporal, disminuyendo significativamente las prestaciones del sistema.

throughput. Caudal. Cantidad real de información por segundo que fluye en una conexión de red, desechando la tara (*overhead*) de los protocolos.

throughput testing tools. Herramientas para medir caudal. Herramientas que miden el ancho de banda neto real entre dos puntos de la red.

Time To Live (TTL). Tiempo de vida. El TTL funciona como un freno de emergencia para señalar el tiempo después del cual los datos deberían ser descartados. En redes TCP/IP el TTL es un contador que empieza con cierto valor (tal como 64), y se decrementa en cada salto (travesía por un enrutador). Si el TTL llega a 0, el paquete se descarta. Este mecanismo ayuda a reducir los daños causados por los lazos de enrutamiento. En DNS, el TTL define la cantidad de tiempo que un determinado registro de zona debe ser mantenido antes de actualizarlo. En Squid, el TTL define cuánto tiempo se debe almacenar un objeto antes de volver a buscarlo en el website original.

TKIP: ver ***Temporal Key Integrity Protocol**.*

TNC connector. Un popular conector de rosca utilizado en microondas.

Tor (http://www.torproject.org/). Una herramienta ***onion routing que*** ofrece buena protección contra el análisis de tráfico.

traceroute / tracert. Herramienta de diagnóstico ubicua usada a menudo en conjunción con *ping* para determinar la ubicación de un problema en la red. La versión Unix se llama *traceroute*, mientras que la versión Windows es *tracert*. Ambas usan paquetes ICMP de solicitud de eco que van incrementando el valor del TTL para determinar cuáles enrutadores se están usando para conectar al anfitrión remoto y también muestra las estadísticas de latencia. Otra variante es *tracepath* que usa una técnica similar con paquetes UDP. Ver también: ***mtr***.

traction batteries: ver ***lead-acid batteries**.*

Transmission Control Protocol (TCP). Protocolo orientado a sesión que opera en la capa de transporte, suministrando reensamblado de paquetes, manejo de la congestión y entrega confiable. TCP es un protocolo integral usado por muchas aplicaciones de Internet incluyendo HTTP y SMTP. Ver también: ***UDP***.

transmission power. Potencia de transmisión. Potencia eléctrica a la salida del transmisor de radio, antes de la ganancia de antena, o de las pérdidas de la línea de transmisión.

transparent bridging firewall. Cortafuego puente-transparente.Técnica de cortafuego que introduce un puente y reenvía selectivamente los paquetes basada en las reglas del cortafuego. Una ventaja del cortafuego puente-transparente es que no requiere una dirección IP. Ver también: ***bridge***.

transparent cache. ***Caché transparente.*** Método de implementar una caché que sirva a toda una organización y que no requiere configuración en las máquinas clientes. Las solicitudes al web se redireccionan automáticamente a la caché, la cual se encarga de procesarlas. Las cache transparentes no pueden utilizar autenticación, lo que hace imposible implementar contabilidad de tráfico en el nivel del usuario. Ver también: ***site-wide web cache***, ***Squid***.

transparent proxy. Proxy transparente. Un *proxy* instalado de manera que las solicitudes al web sean redireccionadas automáticamente al servidor *proxy*, sin necesidad de configurar los navegadores de las máquinas de los usuarios.

transport layer. Capa de transporte. Tercera capa de los modelos de redes ISO y TCP/IP, que provee un método para utilizar un servicio específico en un nodo de la red dado. Los ejemplos más comunes de protocolos de esta capa son ***TCP y UDP***.

trending. Tipo de herramienta que realiza monitoreo sobre largos periodos, y registra los resultados en una gráfica. Las herramientas *trending* le permiten predecir el comportamiento futuro de su red, lo que ayuda en la planificación de actualizaciones y cambios.

TTL: ver ***Time To Live***.

tunnel. ***Tunel***. Una forma de encapsulación que envuelve una pila de protocolos dentro de otra, usada a menudo en conjunción con cifrado para proteger la comunicación contra usuarios no autorizados, eliminando así el requerimiento de que la propia aplicación soporte el cifrado. Los túneles se usan frecuentemente en combinación con ***VPN***.

U

U.FL. Diminuto conector de microondas utilizado por muchas tarjetas de radio mini-PCI.

UDP: ver ***User Datagram Protocol***.

unintentional users. Usuarios no intencionales. Usuarios de Laptops que accidentalmente se asocian a una red inalámbrica equivocada.

Unshielded Twisted Pair (UTP). Par trenzado no apantallado. Cable usado para Ethernet 10baseT y 100baseT, que consiste de cuatro pares de hilos trenzados.

Useful Capacity (Cu). Capacidad usable. Capacidad utilizable de una batería, correspondiente al producto de la ***Capacidad nominal*** y la ***Profundidad máxima de descarga***.

User Datagram Protocol (UDP). Protocolo de la capa de transporte que no utiliza conexión usado comúnmente para audio y video de flujo continuo.

UTP: ver ***Unshielded Twisted Pair***.



valve regulated lead acid battery (VRLA): ver ***lead-acid batteries***.

vertical polarization. Polarizacion Vertical. Campo electromagnético en el que el campo eléctrico se mueve en una dirección lineal vertical. La mayoría de los dispositivos inalámbricos para consumidores utilizan polarización vertical. Ver también: ***circular polarization, horizontal polarization***.

Very Small Aperture Terminal (VSAT). Una de las muchas tecnologías utilizadas para acceso a Internet satelital. VSAT es la tecnología de acceso satelital mas difundida en África y en Latinoamérica. Ver también: ***Broadband Global Access Network (BGAN)*** y ***Digital Video Broadcast (DVB-S)***.

video sender. Transmisor de video a 2,4 GHz; puede ser utilizado como ***generador de señales*** de bajo costo.

Virtual Private Network (VPN). Herramienta utilizada par unir dos redes a través de una tercera no confiable (tal como la Internet). Las VPN se usan a menudo para que los usuarios remotos puedan tener acceso a la red de la organización cuando están viajando, o desde sus hogares. Las VPN utilizan una combinación de túneles y cifrado para asegurar todo el tráfico de red, independientemente de la aplicación que se esté usando. Ver también: ***tunnel***.

VoIP (***Voice over IP***). Tecnología que ofrece servicios similares a los telefónicos sobre una conexión Internet. Ejemplos de clientes populares de VoIP son Skype, Gizmo Project, MSN Messenger, e iChat.

VPN: ver ***Virtual Private Network***.

VRLA: ver ***valve regulated lead acid battery***.

VSAT: ver ***Very Small Aperture Terminal***.



WAN: ver ***Wide Area Network***.

War drivers. Entusiastas de la tecnología inalámbrica que se interesan por encontrar la ubicación física de las redes WiFi.

wavelength. Longitud de onda. La distancia desde un punto en una onda hasta su parte equivalente en la siguiente, por ejemplo desde un pico positivo hasta el siguiente. Se suele representar por la letra griega ***lambda (λ)***.

WEP: ver ***Wired Equivalent Privacy***.

wget. Herramienta de fuente abierta para descargar páginas web: http://www.gnu.org/software/wget/.

Wi-Fi. Marca comercial de propiedad de la WiFi Alliance usada para referirse a las tecnologías 802.11a, 802.11b, y 802.11g. Wi-Fi es la abreviación de ***Wireless Fidelity***.

Wi-Fi Protected Access (WPA). Protocolo de cifrado bastante robusto que opera en la capa de enlace soportado por la mayor parte de los dispositivos Wi-Fi modernos.

Wi-Spy. Dispositivo para análisis de espectro de bajo costo para la banda de 2,4 GHz. Ver http://www.metageek.net/.

Wide Area Network (WAN). Red de área extensa. Cualquier tecnología de redes de larga distancia, tales como líneas dedicadas, *frame relay*, DSL, inalámbrico fijo y servicios vía satélite. Ver también: ***LAN***.

wiki. Sitio web que permite que cualquier usuario edite el contenido de cualquier página. Uno de los mas populares *wiki* públicos es http://www.wikipedia.org/.

window scale. Extensión de TCP definido en RFC1323 que permite tamaños de ventana superiores a 64 kB.

WinDump. Versión Windows de tcpdump disponible en http://www.winpcap.org/windump/.

Wired Equivalent Privacy (WEP). Protocolo de cifrado en la capa de enlace que ofrece cierto grado de seguridad soportado por prácticamente todos los equipos 802.11a/b/g.

Wireless Fidelity: ver ***Wi-Fi***.

wireshark. Analizador de protocolos open source para Linux, Unix , Mac y Windows. http://www.wireshark.org/.

WPA: ver ***Wi-Fi Protected Access***

Z

Zabbix (*http://www.zabbix.org/*). Herramienta de monitoreo en tiempo real que registra y notifica al administrador del sistema las fallas de red y de los servicios.

APÉNDICES

APÉNDICE A: CONSTRUCCIÓN DE ANTENAS

Instrucciones para construir tipos sencillos de antenas

Omni colineal

Esta antena es muy sencilla de armar; sólo se necesita un pedazo de alambre, un conector tipo N y una placa metálica cuadrada. Puede usarse para una cobertura punto a multipunto de corta distancia, en interiores o exteriores. La placa tiene un agujero perforado en el medio para colocar el chasis del conector tipo N, el cual se atornilla en el lugar. El alambre se suelda en la clavija del conector N y tiene espiras para 'desfasar' los elementos activos.

Se pueden hacer dos versiones de la antena: una con dos elementos activos y dos espiras, y otra con cuatro elementos activos y cuatro espiras. Para la antena más corta, la ganancia ronda los 5 dBi, mientras que la más larga, con cuatro elementos, va a tener de 7 a 9 dBi de ganancia. Sólo vamos a describir cómo construir la antena larga.

Componentes y herramientas

- Un conector hembra tipo N de rosca
- 50 cm de alambre de bronce o de cobre de 2 mm de diámetro
- Una placa metálica cuadrada de 10 x 10 cm, o más grande
- Regla
- Pinzas
- Lima
- Estaño y soldador
- Taladro con un juego de mechas para metal, incluyendo una mecha de 1,5 cm de diámetro
- Un pedazo de tubo (caño) o una mecha con un diámetro de 1 cm
- Prensa o abrazadera
- Martillo
- Llave inglesa



Figura CA 1: Placa de aluminio de 10 cm x 10 cm

Construcción

Enderece el alambre utilizando la prensa



Figura CA 2: Deje el alambre tan recto como le sea posible

Con un marcador, dibuje una línea a 2,5 cm comenzando desde uno de los extremos del alambre. En esa línea doble el alambre a 90 grados con la ayuda de la prensa y el martillo.



Figura CA 3: Golpee con delicadeza el alambre para hacer una curva cerrada

Dibuje otra línea a una distancia de 3,6 cm desde la curva anterior. Con la prensa y el martillo, doble otra vez el alambre en esta segunda línea a 90 grados en la dirección opuesta a la primera curva, pero en el mismo plano. El alambre debe verse como una “Z”.





Figura CA 4: Doble el alambre en forma de “Z”

Vamos a retorcer la porción “Z” del alambre para hacer un anillo de 1 cm de diámetro.

Para esto, vamos a utilizar el tubo o la mecha y curvamos el alambre a su alrededor, con la ayuda de la prensa y de las pinzas.





Figura CA 5: Curvar el alambre alrededor de un tubo para hacer un anillo

El anillo va a verse así:



Figura CA 6: El anillo listo

Debe hacer un segundo anillo a una distancia de 7,8 cm desde el primero. Ambos anillos deben tener la misma dirección de giro y deben colocarse alineados del mismo lado del alambre.

Haga un tercer y cuarto anillo siguiendo el mismo procedimiento, y a la misma distancia de 7,8 cm cada uno del otro. Corte el último elemento activo a una distancia de 8,0 cm desde el cuarto anillo.



Figura CA 7: Trate de mantenerlo tan derecho como pueda

Si los anillos fueron hechos correctamente, ahora debe ser posible insertar un tubo a través de todos ellos como se muestra en la imagen.

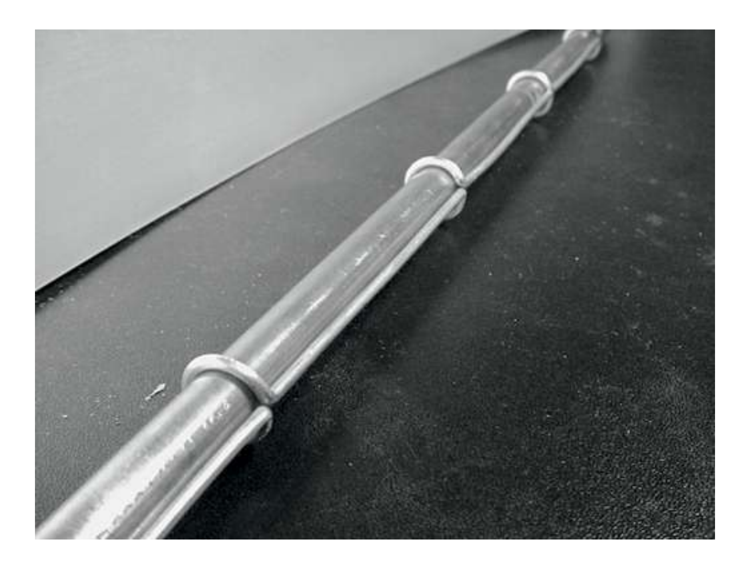


Figura CA 8: Insertar un tubo puede ayudar a enderezar el alambre

Con un marcador y una regla, dibuje las diagonales en la placa metálica para encontrar su centro.
Con una mecha pequeña, haga un agujero piloto en el centro de la placa. Incremente el diámetro del agujero utilizando mechas de mayor diámetro.





Figura CA 9: Taladrar el agujero en la placa de metal

El conector N debe encajar exactamente en la perforación. Si es necesario, use una lima.



Figura CA 10: El conector N debe encajar exactamente en la perforación

Para tener una impedancia de antena de 50 Ohms es importante que la superficie visible del aislante interno del conector (el área blanca alrededor de la clavija central) esté al mismo nivel que la superficie de la placa.

Por esta razón, debe cortar 0,5 cm de un tubo de cobre con un diámetro externo de 2 cm, y colocarlo entre el conector y la placa.



Figura CA 11: Agregar un tubo de cobre espaciador ayuda a obtener la impedancia de la antena de 50 Ohms

Atornille la tuerca al conector para fijarlo firmemente en la placa utilizando la llave inglesa.



Figura CA 12: Asegure el conector N firmemente a la placa

Pula con la lima el lado del alambre que tiene 2,5 cm de largo desde el primer anillo. Cubra de estaño aproximadamente 0,5 cm en el extremo pulido ayudándose con la prensa.

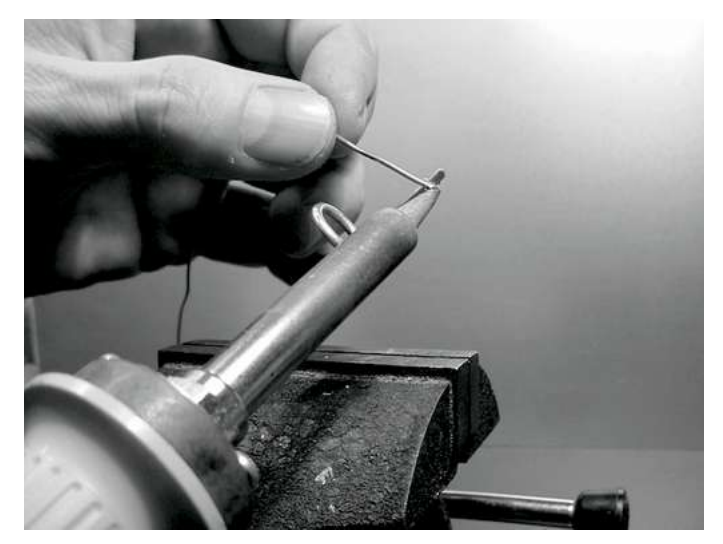


Figura CA 13: Agregue una pequeña capa de estaño al extremo del alambre antes de soldarlo

Con el soldador, estañe la clavija del conector. Mantenga el alambre en posición vertical con las pinzas y suelde el lado con estaño en la clavija. El primer anillo debe estar a 3,0 cm de la placa.



Figura CA 14: El primer anillo debe comenzar a 3,0 cm desde la superficie de la placa

Ahora vamos a estirar los anillos extendiendo el largo total del alambre.

Usando la prensa y las pinzas, estire el alambre hasta que el largo final de cada anillo sea de 2,0 cm.



Figura CA 15: Estirar los anillos con mucho cuidado para no raspar la superficie del alambre con las pinzas

Repita el mismo procedimiento para los otros tres anillos, llevando su longitud a 2,0 cm.

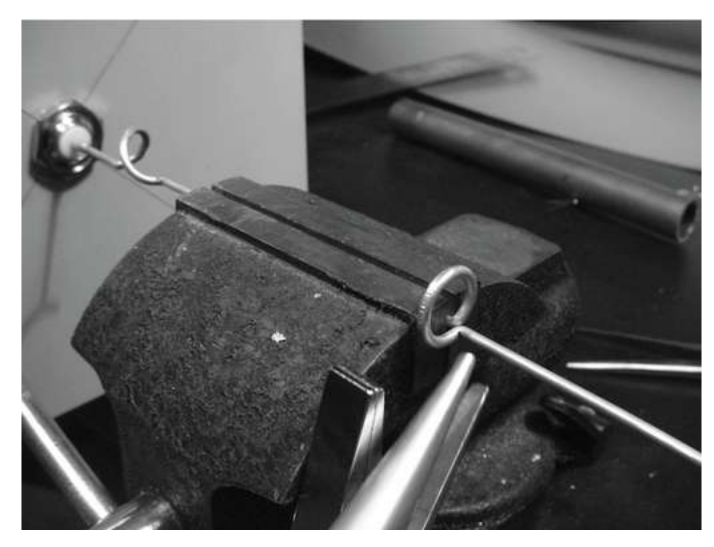


Figura CA 16: Repita el procedimiento de ajuste para todos los anillos restantes

Al terminar, la antena debe medir 42,5 cm desde la placa hasta la punta.

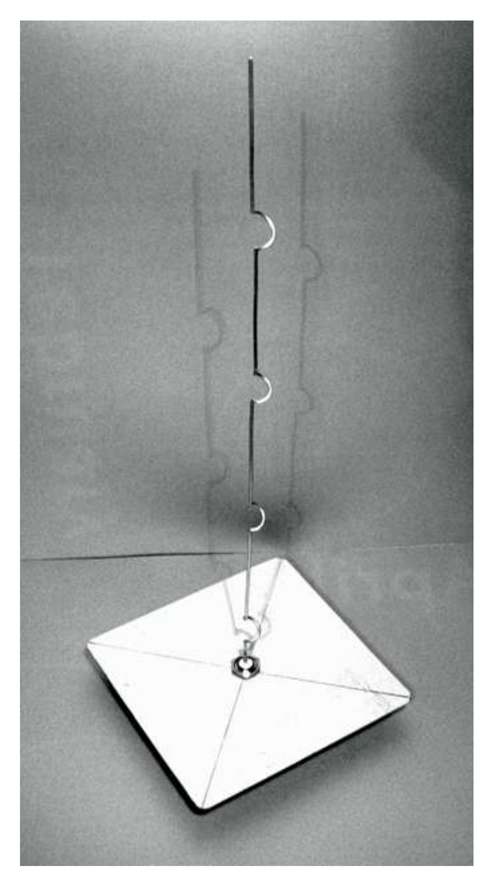


Figura CA 17: La antena terminada debe medir 42,5 cm desde la placa hasta el final del alambre

Si tiene un analizador de espectro con un generador de barrido y un acoplador direccional, puede chequear la curva de la potencia reflejada de la antena. La imagen que sigue muestra la pantalla del analizador de espectro.

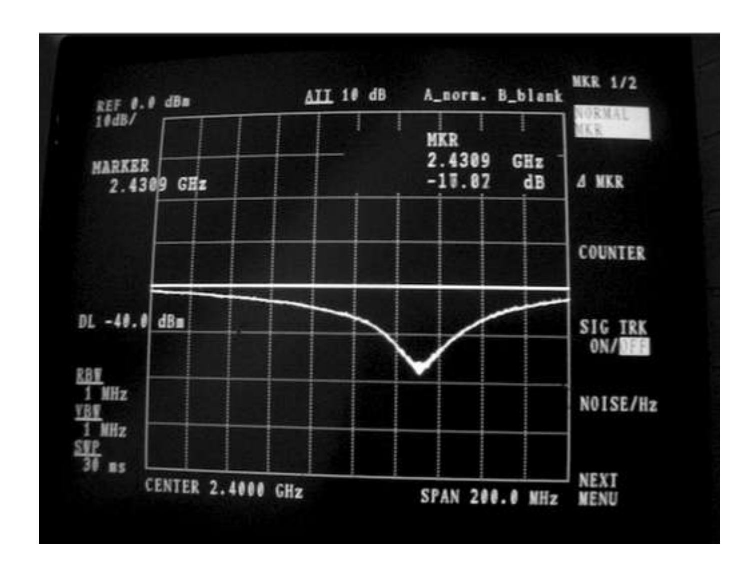


Figura CA 18: Un trazado del espectro de la potencia reflejada por la antena omni colinear

Si quiere utilizar esta antena en exteriores, va a necesitar impermeabilizarla. Un método simple es encerrar toda la antena en un tubo de PVC cerrado con tapas. Abra una perforación abajo para la línea de transmisión y selle la antena con silicona o pegamento.

Antena de lata o de guía-onda

Esta antena algunas veces llamada Cantenna (del inglés *can*: lata), utiliza una lata como guía de onda y un cable corto soldado a un conector N como sonda para la transición del cable coaxial a la guía de onda. Puede construirse fácilmente al precio del conector únicamente, reciclando una lata de comida, de jugo o cualquier otra. Es una antena direccional, útil para enlaces punto a punto de corta a media distancia. También puede utilizarse como alimentador para un plato o una malla parabólica. No todas las latas son buenas para construir una antena porque hay algunas limitaciones en cuanto a la dimensión:

1. Los valores aceptables para el diámetro D del alimentador están entre 0,60 y 0,75 de longitud de onda en el aire a la frecuencia designada. A 2.44 GHz la longitud de onda λ es de 12,2 cm, por lo tanto, el diámetro de la lata debe estar en el rango de 7,3 a 10 cm.

2. El largo L de la lata debería ser preferiblemente de al menos 0,75 λG , donde λG es la longitud de onda dentro de la guía y está dada por:

$\lambda_G = \lambda/(sqrt(1 - (\lambda / 1.706D)^2))$

Cuando D sea = 7,3 cm, necesitaremos una lata de al menos 56,4 cm, mientras que para D = 9,2 cm la lata debería ser de al menos 14,8 cm. Generalmente cuanto más pequeño el diámetro, más larga debe ser la lata. Por ejemplo, vamos a usar latas de aceite que tienen un diámetro de 8,3 cm y una altura de aproximadamente 21 cm.
3. El elemento activo para la transición del cable coaxial a la guía de onda debe posicionarse a una distancia S desde el fondo de la lata, dada por:

$S = 0.25\, \lambda_G$

Su largo debe ser de 0,25 λ, el cual, a 2.44 GHz, corresponde a 3,05 cm.

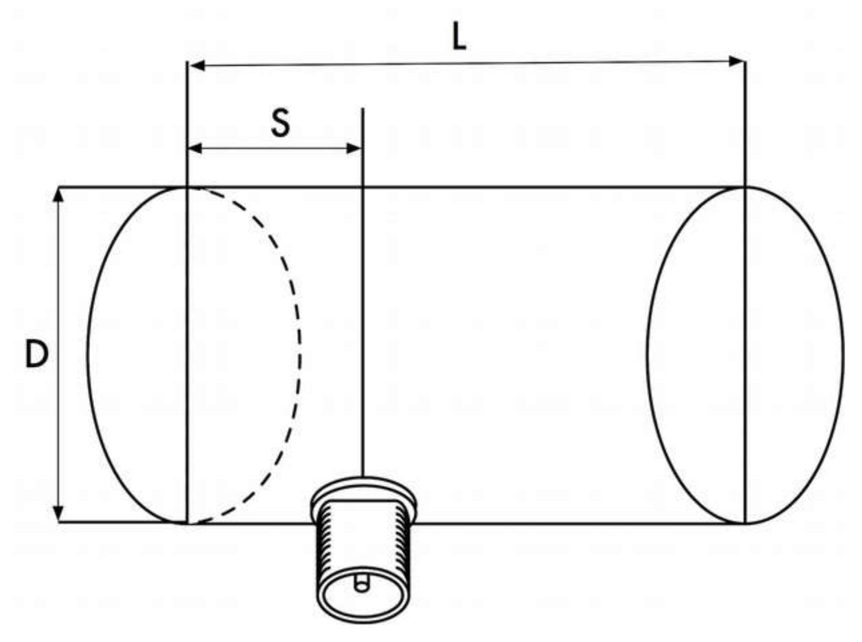


Figura CA 19: Limitaciones de dimensión en la antena guía-onda

La ganancia para esta antena va a estar en el orden de 10 a 14 dBi, con un ancho de haz de alrededor de 60 grados. T



Figura CA 20: La antena guía-onda terminada

Lista de componentes

- un conector hembra tipo N de rosca
- 4 cm de alambre de bronce o de cobre de 2 mm de diámetro
- una lata de aceite de 8,3 cm de diámetro y 21 cm de largo



Figura CA 21: Componentes necesarios para la antena de lata

Herramientas

- Abrelatas
- Regla
- Pinzas
- Lima
- Soldador
- Estaño
- Taladro con un juego de mechas para metal (con una mecha de 1,5 cm de diámetro)
- Prensa o abrazadera
- Llave inglesa
- Martillo
- Perforadora/sacabocados

Construcción

Con el abrelatas quite con cuidado la parte superior de la lata.



Figura CA 22: Cuidado con las puntas afiladas cuando abra la lata

El disco circular tiene puntas muy afiladas. ¡Cuidado al manipularlo! Vacíe la lata y lávela con jabón. Si la lata contenía ananás, galletitas, u otras cosas sabrosas, compártalas.

Con la regla, mida 6,2 cm desde el fondo de la lata y dibuje un punto. Tenga cuidado de medir desde el lado interior del fondo. Utilice una perforadora (o un pequeño taladro, o un destornillador Phillips) y un martillo para marcar el punto. Esto hace que sea más sencillo taladrar el agujero de forma precisa. Asegúrese de no deformar la lata insertando un pequeño bloque de madera u otro objeto dentro de la lata antes de golpearla.



Figura CA 23: Marque el agujero antes de taladrar

Con una mecha pequeña del taladro, haga un agujero en la posición previamente marcada. Incremente el diámetro del mismo utilizando mechas con un diámetro cada vez mayor. El conector N debe encajar exactamente en la perforación. Use la lima para alisar el borde del agujero y remover la pintura que lo rodea para asegurar un mejor contacto eléctrico con el conector.





Figura CA 24: Taladre con cuidado un agujero piloto, luego use una mecha más grande para terminar el trabajo

Alise con la lima uno de los extremos del alambre. Cubra con estaño el alambre alrededor de 0,5 cm en el mismo extremo ayudándose con la prensa.



Figura CA 25: Estañe el extremo del alambre antes de soldarlo

Con el soldador, suelde la clavija del conector. Manteniendo el alambre en posición vertical con las pinzas, suelde el lado estañado en el agujero de la clavija



Figura CA 26: Suelde el alambre a la copa dorada del conector N

Inserte una arandela y atornille suavemente la tuerca en el conector. Recorte el alambre a 3,05 cm medidos desde la base de la tuerca.

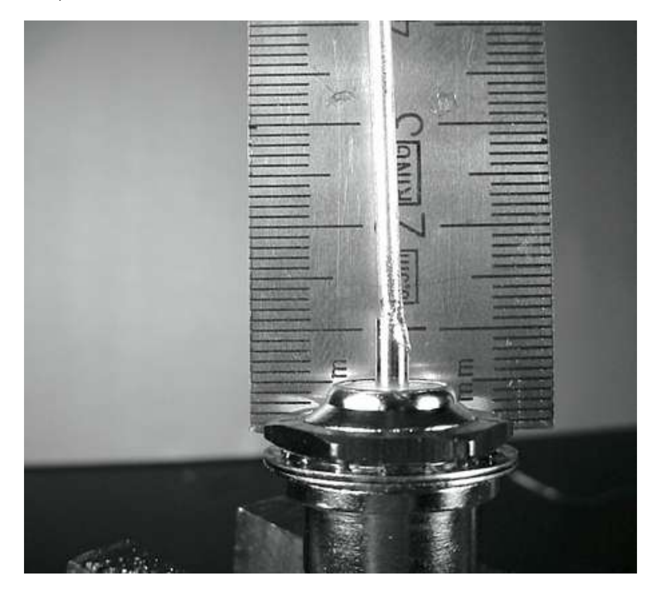


Figura CA 27: El largo del alambre es crucial

Destornille la tuerca del conector, dejando la arandela en el lugar. Inserte el conector en el agujero de la lata. Atornille la tuerca al conector desde el interior de la lata.



Figura CA 28: Arme la antena

Utilice las pinzas o la llave inglesa para ajustar firmemente la tuerca al conector. ¡Ha terminado!



Figura CA 29: Su antena guía-onda terminada

Al igual que los otros diseños de antenas, debe hacer una cubierta a prueba de agua para la antena si quiere usarla en exteriores. El PVC funciona bien para la antena de lata. Coloque toda la antena en un tubo grande de PVC, y selle los extremos con tapas y pegamento. Va a tener que hacer una perforación en un lado del tubo en el lado de la lata para pasar el conector N con la línea de transmisión.

La antena de lata como alimentador de plato

Al igual que con la parabólica con dongle USB, se puede utilizar el diseño antena de lata como un alimentador para obtener una ganancia significativamente mayor.

Monte la antena de lata en la parabólica con el lado abierto de la lata enfocando al centro del plato.

Use la técnica descrita en el ejemplo de la antena dongle USB (observe cómo cambia la intensidad de la señal variando la posición del iluminador) para encontrar la ubicación óptima de la lata para el plato que está usando.

Con el uso de una antena de lata bien construida en una parabólica afinada correctamente, puede lograr una ganancia global de la antena de 30dBi o más. Al incrementar el tamaño de la parabólica, se aumenta la ganancia y la directividad de la antena. Con parábolas muy grandes, puede obtener una ganancia mucho más grande.

NEC2

El NEC2, nombrado así por Numerical Electromagnetics Code, es un paquete de modelación de antenas gratuito. NEC2 le permite construir un modelo de antena en 3D, y luego analiza la respuesta electromagnética de la misma. Fue desarrollado hace más de diez años y ha sido compilado para funcionar en diferentes sistemas de computadoras.

NEC2 es particularmente efectivo para analizar modelos basados en configuraciones de alambres, pero también tiene ciertas facilidades para modelar superficies planas.

El diseño de la antena se describe en un archivo de texto, y luego se construye el modelo utilizando esa descripción textual. Una antena descrita en NEC2 está dada en dos partes: su estructura y una secuencia de controles.

La estructura es simplemente una descripción numérica de dónde se localizan las diferentes partes de la antena y cómo están conectados los alambres. Los controles le dicen a NEC dónde está conectada la fuente de RF. Una vez definidos, se modela la antena transmisora. Debido al teorema de reciprocidad, el patrón de ganancia de transmisión es el mismo que el de recepción, por lo tanto modelar las características de transmisión es suficiente para comprender el comportamiento de la antena en su totalidad.

Se debe especificar una frecuencia o rango de frecuencias de la señal de RF. El siguiente elemento importante son las características del terreno. La conductividad de la tierra varía mucho de lugar a lugar, pero en muchos casos juega un rol vital en determinar el patrón de ganancia de la antena.

Para ejecutar NEC2 en Linux, instale el paquete NEC2 desde el URL que está abajo. Para iniciarlo, escriba nec2 e ingrese los nombres de los archivos de entrada y de salida. También vale la pena instalar el paquete **xnecview** para verificar la estructura y el trazado del patrón de radiación.

Si todo funciona bien debe obtener un archivo que contiene el resultado.

Este puede separarse en varias secciones, pero para una rápida idea de lo que representa se puede trazar un patrón de ganancia utilizando **xnecview**. Usted debería ver el patrón esperado: omnidireccional horizontalmente con un pico correspondiente al ángulo óptimo de salida. También están disponibles las versiones Windows y Mac.

La ventaja de NEC2 es que podemos tener una idea de cómo funciona la antena antes de construirla y cómo podemos modificar el diseño para tener la ganancia máxima posible. Es una herramienta compleja y requiere algo de investigación para aprender a utilizarla efectivamente, pero es invaluable para los diseñadores de antenas.

NEC2 se encuentra en: http://www.nec2.org/

APÉNDICE B: ASIGNACIÓN DE CANALES

Las siguientes tablas listan los números de los canales y frecuencias centrales utilizadas para 802.11a y 802.11b/g.

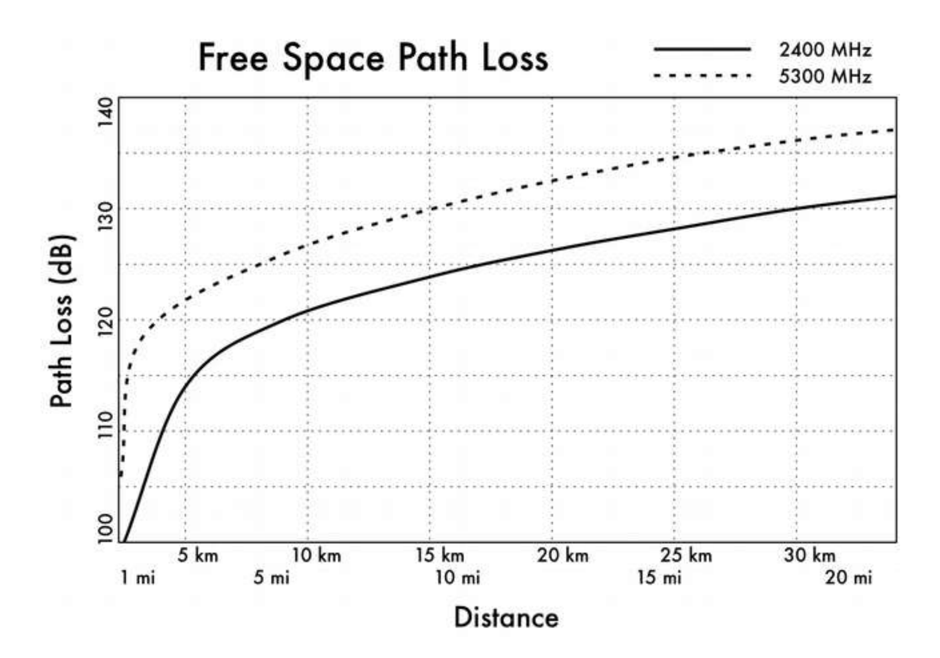
Si bien todas estas frecuencias están en las bandas sin licenciamiento ISM y U-NII, no todos los canales están disponibles en los diferentes países. Muchas regiones imponen restricciones en la potencia de salida y el en uso interiores / exteriores de algunos canales.

Esas regulaciones cambian rápidamente, por lo tanto revise las regulaciones locales antes de transmitir. Estas tablas le muestran la frecuencia central de cada canal. Los canales son de un ancho de 22 MHz en 802.11b/g, y de 20 MHz en 802.11a.

802.11b / g			
# Canal	Frecuencia Central (GHz)	# Canal	Frecuencia Central (GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442	14	2.484

802.11a	
Canal	Frecuencia Central (GHz)
34	5.170
36	5.180
38	5.190
40	5.200
42	5.210
44	5.220
46	5.230
48	5.240
52	5.260
56	5.280
60	5.300
64	5.320
149	5.745
153	5.765
157	5.785
161	5805

APÉNDICE C: PÉRDIDA DE TRAYECTORIA



Free Space Path Loss: Pérdida de Trayectoria en Espacio Libre
Distance: Distancia
Path Loss (dB): Pérdida de Trayectoria (dB)

APÉNDICE D: TAMAÑO DE LOS CABLES

Calibre, diámetro, capacidad máxima y resistencia a 20^0 C. Estos valores pueden variar de cable a cable. Cuando tenga duda, consulte las especificaciones del fabricante. (AWG: *American Wire Gage*)

Calibre AWG	Diámetro (mm)	Ohms / Meter	Amperios Max
0000	11.68	0.000161	302
000	10.40.00	0.000203	239
00	9.27	0.000256	190
0	8.25	0.000322	150
1	7.35	0.000406	119
2	6.54	0.000513	94
3	5.83	0.000646	75
4	5.19	0.000815	60
5	4.62	0.001028	47
6	4.11	0.001296	37
7	3.67	0.001634	30
8	3.26	0.002060	24
9	2.91	0.002598	19
10	2.59	0.003276	15

APÉNDICE E: ENERGÍA SOLAR: DIMENSIONAMIENTO

Use estas tablas para recolectar los datos necesarios para estimar el tamaño de su sistema de energía solar.

Datos Generales

Nombre del Sitio	
Latitud del Sitio (°)	

Datos de Irradiación

$G_{dm}(0)$, en kWh / m² por día

Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Peor Mes de Irradiación											

Confiabilidad y Voltaje Operacional del Sistema

Días de Autonomía (N)	
Voltaje Nominal (V_{NEquip})	

Características de los Componentes

Paneles Solares	
Voltaje @ MáximaPotencia (V_{pmax})	
Corriente @ MáximaPotencia (I_{pmax})	
Tipo de Panel/Modelo y Potencia (W_p)	
Baterías	
Capacidad Nominal @ 100 H (C_{NBat})	
Voltaje Nominal (V_{NBat})	
Profundidad Máxima de Descarga (DoD_{MAX}) o Capacidad Utilizable (C_{UBat})	
Regulador	
Voltaje Nominal (V_{NReg})	
Corriente Máxima (I_{maxReg})	

Paneles Solares	
Voltaje @ MáximaPotencia (V_{pmax})	
Corriente @ MáximaPotencia (I_{pmax})	
Tipo de Panel/Modelo y Potencia (W_p)	
Inversor DC/AC (si se necesita)	
Voltaje Nominal (V_{NConv})	
Potencia Instantánea (P_{IConv})	
Desempeño @ 70% Carga	

Carga

Energía Estimada Consumida por las Cargas (AC)				
Mes de Mayor Consumo				
Descripción	# de Unidades	x Potencia Nominal	x Uso Horas / Día	= Energía (Wh/día)

Energía Estimada Consumida por las Cargas (AC)				
Mes de Mayor Consumo				
E_{TOTAL}^{DC}				
Energía Estimada Consumida por las Cargas (AC)				
Mes de Mayor Consumo				
Descripción	# de Unidades	x Potencia Nominal	x Uso Horas / Día	= Energía (Wh/día)

Energía Estimada Consumida por las Cargas (AC)				
Mes de Mayor Consumo				
E_{TOTAL} AC (antes del conversor)				
E_{TOTAL} AC (después del conversor) = E_{TOTAL} AC / 70%				

Cómo Encontrar el Peor Mes

Nombre del Sitio												
Latitud del Sitio (°)												
Voltaje Nominal de la Instalación V_N												
(Mes)	E	F	M	A	M	J	J	A	S	O	N	D
Inclinación ß												
G_{dm} (ß) (kWh/m^2 × día)												

Nombre del Sitio												
Latitud del Sitio (°)												
ETOTAL (DC) (Wh/día)												
ETOTAL (AC) (Wh/día)												
ETOTAL (AC + DC)=												
I_m (A) = ETOTAL (Wh/día) × 1kW/m^2/ (G_{dm}(ß) x V_N)												
Resumen del Peor Mes												
Peor Mes												
I_m (A)												
I_mMAX (A) = 1.21 x I_m												
ETOTAL (AC + DC)												

Cálculos Finales

Paneles			
Paneles en Serie (N_{PS})	$N_{PS} = V_N / V_{Pmax} =$		
Paneles en Paralelo (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax} =$		
Número Total de Paneles	$N_{TOT} = N_{PS} \times N_{PP} =$		
Baterías			
Capacidad Necesaria (C_{NEC})	$E_{TOTAL}(PEOR\ MES) / V_N \times N$		
Capacidad Nominal (C_{NOM})	C_{NEC} / DoD_{MAX}		
Número de Baterías en Serie (N_{BS})	V_N / V_{NBAT}		
Cables			
	Paneles > Baterías	Baterías > Conversor	Línea Principal
Caída de Voltaje (V_a - V_b)			

Paneles			
Paneles en Serie (N_{PS})	$N_{PS} = V_N / V_{Pmax} =$		
Paneles en Paralelo (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax} =$		
Espesor (Sección) $r \times L \times I_{mMAX} / (V_a - V_b)$			

Para el cálculo del espesor, r = 0.01286 Ω mm^2/m (para cobre) y L es la longitud en metros.

APÉNDICE F: RECURSOS

Recomendamos estos recursos para que quienes así lo deseen puedan aprender más acerca de los variados aspectos de las redes inalámbricas. Estos están disponibles solamente en inglés. Si quiere conocer más enlaces y recursos, visite nuestro sitio web en http://wndw.net/ y el exhaustivo http://wirelessU.org.

Para materiales **en español** visite http://www.eslared.org.ve.

Antenas y Diseño de Antenas

Free antenna designs, http://www.freeantennas.com/
Hyperlink Tech, http://hyperlinktech.com/
Pasadena Networks LLC, http://www.wlanparts.com/
SuperPass, http://www.superpass.com/
Unofficial NEC2 code archives, http://www.nec2.org/
USB WiFi dish designs, http://www.usbwifi.orcon.net.nz/

Herramientas para Diagnóstico de Problemas de Redes

Bing throughput measurement tool,http://fgouget.free.fr/bing/index-en.shtml
Cacti network monitoring package, http://www.cacti.net/
DSL Reports bandwidth speed tests, http://www.dslreports.com/stest EtherApe network traffic monitor, http://etherape.sourceforge.net/
Flowc open source NetFlow collector, http://netacad.kiev.ua/flowc/
iptraf network diagnostic tool, http://iptraf.seul.org/
My TraceRoute network diagnostic tool, http://www.bitwizard.nl/mtr/
Nagios network monitoring and event notification tool, http://www.nagios.org/
NetFlow, the Cisco protocol for collecting IP traffic information, http://en.wikipedia.org/wiki/Netflow
ngrep network security utility for finding patterns in data flows, http://ngrep.sourceforge.net/
Network monitoring implementation guides and tutorials, http://wiki.debian.org/Network_Monitoring
Ntop network monitoring tool, http://www.ntop.org/
SoftPerfect network analysis tools, http://www.softperfect.com/
Squid transparent http proxy HOWTO, http://tldp.org/HOWTO/TransparentProxy.html
Wireshark network protocol analyzer, http://www.wireshark.org/
MRTG, http://oss.oetiker.ch/mrtg/
rrdtool, http://oss.oetiker.ch/rrdtool/
Smokeping, http://oss.oetiker.ch/smokeping/

Argus, http://qosient.com/argus/
Netramet, http://www.caida.org/tools/measurement/netramet/
Snort, http://www.snort.org/
Mod Security, http://www.modsecurity.org/
Apache, http://www.apache.org/
Zabbix, http://www.zabbix.org/
ngrep, http://ngrep.sourceforge.net/
nmap, http://www.nmap.org
netcat, http://nc110.sourceforge.net/

Seguridad

AntiProxy http proxy circumvention tools and information, http://www.antiproxy.com/
Anti-spyware tools, http://www.spychecker.com/
Driftnet network monitoring utility, http://www.exparrot.com/~chris/driftnet/
Introduction to OpenVPN, http://www.linuxjournal.com/article/7949
Linux security and admin software, http://www.linux.org/apps/all/Networking/Security_/_Admin.html
OpenSSH secure shell and tunneling tool, http://openssh.org/
OpenVPN encrypted tunnel setup guide, http://openvpn.net/howto.html
Privoxy filtering web proxy, http://www.privoxy.org/
PuTTY SSH client for Windows, http://www.putty.nl/
Sawmill log analyzer, http://www.sawmill.net/
Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
Stunnel Universal SSL Wrapper, http://www.stunnel.org/
TOR onion router, http://www.torproject.org/
Weaknesses in the Key Scheduling Algorithm of RC4, http://www.crypto.com/papers/others/rc4_ksaproc.ps
Windows SCP client, http://winscp.net/
Your 802.11 Wireless Network has No Clothes, http://www.cs.umd.edu/~waa/wireless.pdf
ZoneAlarm personal firewall for Windows, http://www.zonelabs.com/
Logging, http://wigle.net/, http://www.nodedb.com/,
or http://www.stumbler.net/. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html http://www.cs.umd.edu/~waa/wireless.pdf
http://dl.aircrack-ng.org/breakingwepandwpa.pdf
http://download.aircrackng.org/wikifiles/doc/enhanced_tkip_michael.pdf
Captive Portals, CoovaChilli, CoovaAP (http://coova.org/CoovaChilli/) WiFidog (http://www.wifidog.org/)
M0n0wall, pfSense (http://m0n0.ch/wall/)

Putty, http://www.putty.nl/
Win SCP, http://winscp.net/
Cygwin, http://www.cygwin.com/
OpenVPN Journal, http://www.linuxjournal.com/article/7949
Tor, http://www.torproject.org/
Spychecker, http://www.spychecker.com/

Optimización del Ancho de Banda

Cache hierarchies with Squid, http://squid-docs.sourceforge.net/latest/html/c2075.html
dnsmasq caching DNS and DHCP server, http://www.thekelleys.org.uk/dnsmasq/doc.html
Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies, http://www.isoc.org/inet97/ans97/cloet.htm
Fluff file distribution utility, http://www.bristol.ac.uk/fluff/
Linux Advanced Routing and Traffic Control HOWTO, http://lartc.org/
Microsoft Internet Security and Acceleration Server, http://www.microsoft.com/isaserver/
Microsoft ISA Server Firewall and Cache resource site, http://www.isaserver.org/
Optimising Internet Bandwidth in Developing Country Higher Education, http://www.inasp.info/pubs/bandwidth/index.html
Planet Malaysia blog on bandwidth management, http://planetmy.com/blog/?p=148
RFC 3135: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations, http://www.ietf.org/rfc/rfc3135
Squid web proxy cache, http://squid-cache.org/

Redes en Malla (*Mesh*)

Freifunk OLSR mesh firmware for the Linksys WRT54G, http://www.freifunk.net/wiki/FreifunkFirmware
MIT Roofnet Project, http://pdos.csail.mit.edu/roofnet/doku.php
OLSR mesh networking daemon, http://www.olsr.org/
AirJaldi Mesh Router, http://drupal.airjaldi.com/node/9
Open WRT, http://wiki.openwrt.org/toh/start
Village Telco, www.villagetelco.org

Sistemas Operativos Inálambricos y *Drivers*

DD-WRT wireless router OS,http://www.dd-wrt.com/
HostAP wireless driver for the Prism 2.5 chipset, http://hostap.epitest.fi/
m0n0wall wireless router OS, http://m0n0.ch/wall/
MadWiFi wireless driver for the Atheros chipset, http://madwifi.org/ Metrix

Pyramid wireless router OS, http://code.google.com/p/pyramidlinux/
OpenWRT wireless router OS for Linksys access points, http://openwrt.org/
Tomato wireless router OS for Linksys access points, http://www.polarcloud.com/tomato

Herramientas Inalámbricas

Chillispot captive portal, http://www.chillispot.info/
Interactive Wireless Network Design Analysis Utilities, http://www.qsl.net/n9zia/wireless/page09.html
KisMAC wireless monitor for Mac OS X, http://kismac-ng.org/
Kismet wireless network monitoring tool, http://www.kismetwireless.net/
MacStumbler wireless network detection tool for Mac OS X, http://www.macstumbler.com/
NetStumbler wireless network detection tool for Windows, http://www.wirelessdefence.org/Contents/NetstumblerMain.htm
Netspot wireless network detection for Mac OS X, http://www.netspotapp.com/
PHPMyPrePaid prepaid ticketing system, http://sourceforge.net/projects/phpmyprepaid/
RadioMobile radio performance modeling tool,
http://www.cplus.org/rmw/
Radio Mobile online, http://www.cplus.org/rmw/rmonline.html
Wellenreiter wireless network detection tool for Linux, http://sourceforge.net/projects/wellenreiter/
WiFiDog captive portal, http://www.wifidog.org/
Proxim, http://www.proxim.com/technology
WiSpy spectrum analysis tool, http://www.metageek.net/
Spectrum Analyser, http://www.seeedstudio.com/depot/rf-explorer-model-wsub1g-p-922.html?cPath=174
"RF Explorer model 2.4G",
http://www.seeedstudio.com/depot/-p-924.htmlcPath=174
VideoSend.
http://www.lightinthebox.com/Popular/Wifi_Video_Transmitter.html

Información General sobre Redes Inalámbricas

Homebrew wireless hardware designs, http://www.w1ghz.org/
Linksys wireless access point information, http://linksysinfo.org/
Linksys WRT54G resource guide, http://seattlewireless.net/index.cgi/LinksysWrt54g
Ronja optical data link hardware, http://ronja.twibright.com/
SeattleWireless community wireless group, http://seattlewireless.net/
SeattleWireless Hardware comparison page,

http://www.seattlewireless.net/HardwareComparison
Stephen Foskett's Power Over Ethernet (PoE) Calculator, http://www.gweep.net/~sfoskett/tech/poecalc.html
White Spaces project, http://www.wirelesswhitespace.org/projects.aspx

Herramientas Generales de Computación

File sharing, http://sparkleshare.org, https://github.com/philcryer/lipsync, http://rsync.samba.org/
Open Relay testing, http://www.mailradar.com/openrelay, http://www.checkor.com/
Disk imaging, http://www.partimage.org, http://www.powerquest.com/

Servicios de Redes y Entrenamiento

Wireless Toolkit, http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html
wire.less.dk consultancy and services, http://wire.less.dk/
Wireless Lab and training at ICTP, http://wireless.ictp.it/
WirelessU, http://wirelessu.org/
Network Startup Resource Center, Oregon, http://www.nsrc.org/
Inveneo, http://www.inveneo.org/
6Deploy (EC FP7 project), http://www.6deploy.org
Association for Progressive Communications wireless connectivity projects, http://www.apc.org/wireless/
International Network for the Availability of Scientific Publications, http://www.inasp.info/
Makere University, Uganda, http://mak.ac.ug/
Access Kenya ISP, http://www.accesskenya.com/
Broadband Access Ltd. wireless broadband carrier, http://www.blue.co.ke/
Virtual IT outsourcing, http://www.virtualit.biz/
Collection of looking glasses, http://www.traceroute.org/

Registro Regional de Internet

IANA, http://www.iana.org/
AfriNIC, http://www.afrinic.net/
APNIC, http://www.apnic.net/
ARIN, http://www.arin.net/
LACNIC, http://www.lacnic.net/
RIPE NCC, http://www.ripe.net/

Transición IPv6

http://www.petri.co.il/ipv6-transition.htm
http://www.6diss.org/tutorials/transitioning.pdf
http://arstechnica.com/business/2013/01/ipv6-takes-one-step-forward-ipv4-two-

steps-back-in-2012/
http://www.6deploy.eu/index.php?page=home
RIPE IPv6 transiton, http://www.ipv6actnow.org/
Test your IPv6, http://tet-ipv6.org
IPv6 Deployment status, http://6lab.cisco.com

Protocolos de Enrutamiento Dinámico

http://www.ciscopress.com/store/routing-tcp-ip-volume-i-ccie-professional-development-9781578700417?w_ptgrevartcl=Dynamic%20Routing %20Protocols_24090
http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=5
http://ptgmedia.pearsoncmg.com/images/9781587132063/samplechapter/1587132060_03.pdf
http://www.inetdaemon.com/tutorials/internet/ip/routing/dyamic_vs_static.shtml
https://learningnetwork.cisco.com/docs/DOC-7985
OSPF Design guide: http://www.cisco.com/warp/public/104/1.pdf

Diseño de Paneles Solares

Low resolution PSH maps/calculation tools,
http://re.jrc.ec.europa.eu/pvgis/apps4/pvest.php?map=africa&lang=en
Highlands And Islands project,
http://www.wirelesswhitespace.org/projects/wind-fi-renewable-energy-basestation.aspx
PVSYST, http://www.pvsyst.com/
Solar Design, http://www.solardesign.co.uk/

Enlaces Misceláneos

Cygwin Linux-like environment for Windows, http://www.cygwin.com/ Graphviz network graph visualization tool, http://www.graphviz.org/ ICTP bandwidth simulator, http://wireless.ictp.trieste.it/simulator/ ImageMagick image manipulation tools and libraries, http://www.imagemagick.org/
NodeDB war driving map database, http://www.nodedb.com/
Partition Image disk utility for Linux, http://www.partimage.org/
RFC 1918: Address Allocation for Private Internets, http://www.ietf.org/rfc/rfc1918
Rusty Russell's Linux Networking Concepts,
http://www.netfilter.org/documentation/HOWTO/networkig-concepts-HOWTO.html
Ubuntu Linux, http://www.ubuntu.com/
VoIP-4D Primer, http://www.it46.se/voip4d/voip4d.php
wget web utility for Windows, http://users.ugent.be/~bpuype/wget/
ISO Standard, http://standards.iso.org/ittf/PubliclyAvailableStandards

Libros

802.11 Networks: The Definitive Guide, 2nd Edition. Matthew Gast, O'Reilly Media. ISBN #0-596-10052-3

802.11 Wireless Network Site Surveying and Installation. Bruce Alexander, Cisco Press. ISBN #1-587-05164-8

The ARRL UHF/Microwave Experimenter's Manual. American Radio Relay League. ISBN #0-87259-312-6

Building Wireless Community Networks, 2nd Edition. Rob Flickenger, O'Reilly Media. ISBN #0-596-00502-4

Deploying License-Free Wireless Wide-Area Networks. Jack Unger, Cisco Press. ISBN #1-587-05069-2

Wireless Hacks, 2nd Edition. Rob Flickenger and Roger Weeks, O'Reilly Media. ISBN #0-596-10144-9

IPv6 Security (Cisco Press Networking Technology). Scott Hogg, Eric Vyncke, Cisco Press. ISBN # 1587055945

LAN Switch Security: What Hackers Know About Your Switches. Eric Vyncke and Christopher Paggen. ISBN #1587052563

Building the Mobile Internet. Mark Grayson, Kevin Shatzkamer, Klaas Wierenga. ISBN # 1587142430

ESTUDIO DE CASOS

Introducción

No importa cuánto planeemos el montaje de un enlace o nodo, inevitablemente llega el momento en que tenemos que lanzarnos a instalar algo. Este es el momento de la verdad donde se demuestra cuán acertadas eran nuestras estimaciones y predicciones.

Es muy raro el día en el que todo pasa como lo habíamos planeado. Incluso después de instalar su primer enlace, o el décimo o el centésimo, siempre encontrará que las cosas no siempre funcionan según sus intenciones. Esta sección describe algunos de nuestros trabajos de redes más memorables y recientes. Sea que usted esté a punto de embarcarse en su primer proyecto inalámbrico o sea usted un(a) veterano(a), es siempre reconfortante recordar que todavía se puede aprender algo. Incluso los expertos que han contribuido con este libro aprenden todavía de cada proyecto en los que se involucran.
A continuación les damos unos consejos y reflexiones de última hora antes de contarles sobre nuestras últimas aventuras de campo.

Recipientes para equipos

Los recipientes de plásticos baratos suelen ser fáciles de conseguir pero el material no es bueno y es muy delgado; por lo tanto poco apropiado para proteger equipo. Los tubos de PVC son más resistente y son impermeables. En el oeste de África, el PVC más común se encuentra en los negocios de venta de productos para plomería, con calibres que oscilan entre los 90 a 220mm. A veces los AP pueden caber en estos tubos que sellados con tapas en los extremos crean una cubierta robusta a prueba de agua. También tienen la ventaja de ser aerodinámicos y poco interesantes a los ojos de los transeúntes. Además, el espacio que sobra alrededor del equipo garantiza una buena circulación del aire. También es bueno dejar un agujero de ventilación en el fondo de la cubierta PVC, aunque una vez las hormigas decidieron hacer su nido a 25 m sobre el suelo dentro del tubo de PVC usado para el AP. Un trozo de malla metálica de los usados localmente para rejillas se empleó en este caso para impedir el paso de insectos por el agujero de ventilación.

Mástiles para antenas

Recuperar materiales usados para construir el mástil de la antena es una buena idea. Los trabajadores locales pueden ya estar familiarizados con la construcción de mástiles para televisión de metal de desecho. Con algunas rápidas modificaciones, estos mismos mástiles puede reutilizarse en redes inalámbricas.

Un mástil típico es un poste de 5 metros compuesto por un único tubo de 30mm de diámetro enterrado en el cemento. Es mejor construir el mástil en dos partes con una parte removible que encastra en una base con un diámetro levemente más grande. Como alternativa, el mástil puede hacerse con brazos empotrados a un muro de forma segura. Este tipo de mástil puede alargarse varios metros con la ayuda de cables tensores. Para inmovilizar el poste plante tres líneas separadas 120 grados con una caída de por lo menos 33 grados desde la punta de la torre.
Los detalles sobre cómo enterrar el mástil los puede leer en el capítulo sobre **Selección y Configuración del Hardware.**

Involucrar a la comunidad local

Involucrar a la comunidad es esencial para garantizar el éxito y sostenibilidad de un proyecto y a la vez puede ser el reto más grade. Pero si no lo hace, la tecnología no va a ser útil para la satisfacción de las necesidades de la gente ni va a ser aceptada. Es más, si la comunidad tiene algún temor podría coartar una iniciativa. A pesar de que el asunto sea complejo un proyecto exitoso necesita el respaldo y la credibilidad de aquellos a los que planea prestar sus servicios.

Tómese su tiempo y seleccione con cuidado la gente adecuada para su proyecto. Ninguna decisión lo va a afectar tanto como tener en su equipo gente local eficiente y confiable.

Además, fíjese en las personas que son claves en una institución o comunidad. Identifique la gente que pude ser propulsora u opositora de su proyecto.

Esa es una tarea difícil porque requiere un conocimiento profundo de la institución o comunidad. Si el proyecto no cuenta con un aliado local, debe dedicar algún tiempo para lograr el conocimiento y ganarse la confianza de la comunidad. No trate de introducir una tecnología en una comunidad sin saber antes cuáles aplicaciones serán de utilidad.
Cuando recabe información, verifíquela en la práctica. A veces, los socios locales que tienen confianza en usted le serán francos, honestos y útiles.
Cuando busque métodos de pago para su nuevo servicio inalámbrico, escoja el prepagado ya que no necesita un contrato legal. El compromiso es asegurado por la inversión de fondos antes de que el servicio sea prestado. Cuando se hacen adquisiciones también se requiere que los involucrados inviertan en el proyecto. Siempre se debe pedir el compromiso recíproco de la comunidad.
Cancelar la implementación es una opción que siempre debe considerarse. Si no se puede tener un aliado y una comunidad convencida, el proyecto debe considerar escoger otra comunidad o beneficiario.
En pocas palabras, debe haber una negociación: el equipo, el dinero y el entrenamiento no pueden ser regalos. La comunidad debe involucrarse y sus miembros deben contribuir.

Ahora, siga leyendo

En las próximas secciones de este capítulo encontrará algunos de nuestros proyectos que esperamos puedan dejar alguna enseñanza. No se han incluido estudios de casos de versiones anteriores excepto para el caso de Venezuela que fue fundamental para demostrar la viabilidad de enlaces exteriores de larga distancia punto a punto para conectividad rural.

Un caso de estudio que no se incluye en esta sección fue desarrollado por Inveneo que está trabajando con el equipo comprometido en la producción de este libro. Su descripción está disponible en la URL que se proporciona. El proyecto coordinado por Andris Bjornson, CTO de Inveneo, presenta información muy útil en su descripción.
http://www.inveneo.org/90km-wireless-link-for-mfangano-island/

Esperamos que disfrute con la lectura de cada estudio de caso a continuación en los que se apreciará a quiénes estuvieron involucrados, cuyos perfiles puede leer en los **Agradecimientos** de este libro.
Todos los autores han participado en instalaciones de campo y monitorean nuestra página de Facebook que puede encontrar en:
https://www.facebook.com/groups/wirelessu
Así que si está planeando su próxima instalación no vacile en enviarnos las preguntas que quiere que nuestros expertos le respondan.

Estudio de Casos: Larga Distancia 802.11 en Venezuela

Introducción

Aunque este estudio de caso tiene ya varios años lo hemos incluido en esta versión ya que es la prueba 802.11 del enlace punto a punto para exteriores más largo que se haya realizado con éxito hasta el día de hoy. Se describirá el trabajo pionero de algunos que todavía están contribuyendo con este libro. Y, de hecho, algunos trabajos de preparación para la realización de esta prueba son todavía relevantes para las personas que planifican enlaces exteriores de larga distancia. !Disfruten la lectura!

Antecedentes

Gracias a una topografía favorable, Venezuela ya posee algunos enlaces WLAN de larga distancia, como el de 70 km operado por Fundacite Mérida entre Pico Espejo y Canaguá. Para probar los límites de esta tecnología, es necesario encontrar un trayecto con línea de vista ininterrumpida y despeje de al menos el 60% de la primera zona de Fresnel.

Examinando el terreno en Venezuela en búsqueda de un recorrido con altas elevaciones en los extremos y tierras bajas en el ínterin, me enfoqué primero en la región de Guayana, en la que abundan las elevaciones, en particular los famosos "tepuys" (altas mesetas de paredes verticales), pero siempre había obstáculos en el terreno intermedio. Mi atención se concentró entonces en los Andes, cuyas fuertes pendientes (que se alzan abruptamente desde los llanos) demostraron ser idóneas para el propósito. Durante muchos años, he estado recorriendo las zonas escasamente pobladas gracias a mi pasión por la bicicleta de montaña, manteniéndome ojo avizor sobre la viabilidad de posibles enlaces de larga distancia. El pico del Águila tiene condiciones muy favorables para establecer una estación. Tiene una altura de 4200 m y está a unas dos horas en automóvil de mi residencia en la ciudad de Mérida. Para el otro extremo, luego de examinar muchas posibilidades, finalmente escogí la población de El Baúl, en el estado Cojedes. Usando el software gratuito Radio Mobile (disponible en www.cplus.org/rmw) encontré que no había obstrucción de la primera zona de Fresnel en el tramo de 280 km entre Pico del Águila y el Baúl.

Plan de Acción

Una vez satisfechos con la existencia de una trayectoria adecuada, pasamos a escoger el equipo necesario para alcanzar nuestra meta. Hemos estado usando tarjetas Orinoco desde hace muchos años.

Con una potencia de salida de 15 dBm y umbral de recepción de -84 dBm, son robustas y confiables. La pérdida en el espacio libre a 280 km es de 149 dB, por lo que necesitaríamos antenas de 30 dBi en ambos extremos y aún así el margen para compensar otras pérdidas sería muy reducido.

Por otra parte, el popular enrutador inalámbrico Linksys WRT54G está basado en Linux.

La comunidad del software de fuente abierta ha producido varias versiones de *firmware* que permiten modificar todos los parámetros de transmisión de este dispositivo.

En particular, el *firmware* OpenWRT permite modificar el tiempo de espera de los reconocimientos (ACK) de la capa de acceso al medio, así como la potencia de transmisión. Otro *firmware*, DD-WRT, tiene una interfaz gráfica y ofrece facilidades para prospección de sitios.

Además, el Linksys se puede colocar más cerca de la antena que un laptop, disminuyendo así las pérdidas en el cable de RF, así que decidimos usar una par de estos enrutadores, uno configurado como AP (Access Point) y el otro como cliente.

El WRT54G puede ser operado a 100 mW con buena linealidad, e inclusive llevado a 200 mW, pero a este último valor se generan señales espurias que deben ser evitadas.

Aunque este dispositivo es muy económico y no pretende ser un equipo profesional, lo hemos utilizado por varios años y confiamos que podía servir para nuestros propósitos.

Por supuesto, teníamos un par de repuesto para cualquier eventualidad.

Colocando la potencia de salida a100 mW (20dBm) podíamos obtener una ventaja de 5 dB comparado con las tarjetas Orinoco, por lo que nos decidimos por un par de WRT54G.

Prospección del sitio de Pico del Águila

El 15 de enero de 2006, visité el Pico del Águila para revisar el sitio que según el Radio Mobile era viable. El acimut hacia El Baúl es de 86°, pero puesto que la declinación magnética es de 8°16´, nuestra antena debería apuntarse a un rumbo magnético de 94°.

Desafortunadamente, cuando examiné esa dirección, me encontré con que la línea de vista estaba obstruida por un obstáculo que no había sido detectado por el software, debido a la limitada resolución de los mapas digitales de elevación gratuitos que estaba utilizando.

Recorrí el área circundante durante varias horas en mi bicicleta de montaña, buscando una trayectoria sin obstrucción hacia el este. Logré identificar varios sitios prometedores y para cada uno de ellos tomé fotos y registré las coordenadas con el GPS para luego procesarlos con el software Radio Mobile.

Esto me llevó a refinar mi selección de la trayectoria, resultando la que se muestra en la Figura EcLD 1: usando Google Earth.



Figura EcLD 1: Vista del enlace de 280 km. El lago de Maracaibo al oeste y la Península de Paraguaná al Norte

Los detalles del enlace inalámbrico se muestran en la Figura EcLD 22:

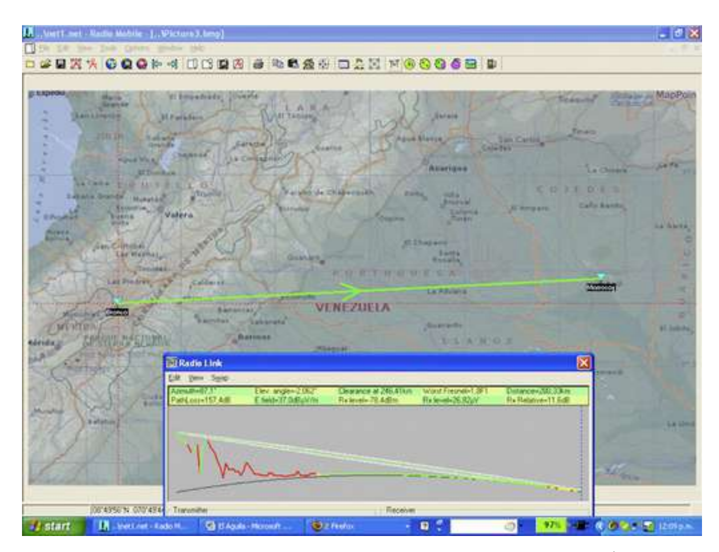


Figura EcLD 2: Mapa y perfil del trayecto entre el Pico del Águila y el cerro Morrocoy, cerca de El Baúl

Los detalles del enlace inalámbrico se muestran en la Figura EcLD 3:

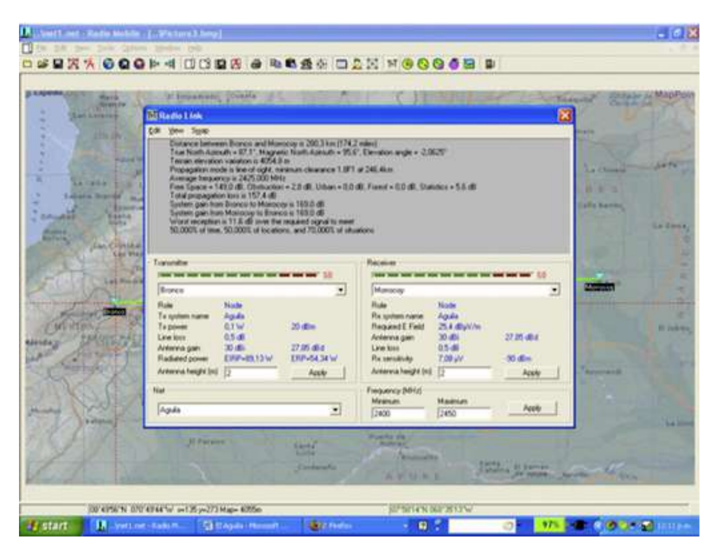


Figura EcLD 3: Detalles de propagación en el trayecto de 280 km

A fin de obtener un margen razonable de unos 12 dB para el enlace, necesitamos antenas de al menos 30 dBi en cada extremo.

Antenas

En Venezuela no venden antenas de alta ganancia para la banda de 2,4 GHz. Los costos de importación son considerables, así que decidimos reciclar reflectores parabólicos (de los usados anteriormente para recepción satelital) reemplazándole el alimentador por uno de 2.4 GHz. Primeramente probamos la viabilidad con un reflector de 80 cm, la ganancia era demasiado baja, por lo que ensayamos con reflector de 2,4 m de diámetro con alimentación excéntrica. Este ofrecía amplia ganancia, a expensas de alguna dificultad en la alineación del haz de 3,5°.

La iluminación excéntrica desviada en 22,5° hacía que el reflector pareciera estar apuntando hacia abajo, cuando estaba alineado horizontalmente. Se hicieron varias pruebas utilizando antenas de guía-onda (*cantenna*) y Yagi de 24 dBi como iluminadores del reflector parabólico. Apuntamos la antena a la estación base de la universidad, a una distancia de 11 km en una montaña de 3500 m de altura. El sitio de prueba está a 2000 m de altura por lo tanto el ángulo de elevación es de 8°. Debido a la iluminación excéntrica, apuntamos el reflector 14° hacia abajo, como se puede apreciar en la siguiente foto:



Figura EcLD 4: Reflector de 2,4 m con iluminación excéntrica y una antena de 12 dBi en su punto focal, mirando 14° hacia abajo. El ángulo real de elevación es de 8° hacia arriba

Logramos conectar con la estación base de la universidad en La Aguada, pero los esfuerzos dirigidos a estimar la ganancia de la antena usando ***Netstumbler*** fueron vanos, ya que los niveles de potencia de la señal recibida correspondiente a tráfico normal fluctuaban considerablemente.

Para poder realizar una medida razonable de la ganancia, se requiere un generador de señales y un analizador de espectros. Los mismos instrumentos son también necesarios en el trabajo de campo para alinear las antenas adecuadamente.

Mientras esperábamos la llegada de estos instrumentos, nos pusimos a buscar la antena a usar en el otro extremo, así como una mejor técnica para alinear las antenas de haz muy estrecho.

En febrero de 2006 viajé a Trieste para participar en el evento anual de entrenamiento en redes inalámbricas con el que he estado colaborando desde 1996. Allí le mencioné el proyecto a mi colega Carlo Fonda que enseguida se mostró entusiasta en participar.

La colaboración entre la **Escuela Latinoamericana de Redes (EsLaRed)** y el ***Abdus Salam International Centre for Theoretical Physics (ICTP)*** data desde 1992 cuando la primera Escuela Latinoamericana de Redes se realizó en Mérida con el apoyo del ICTP.

Desde entonces, los miembros de ambas instituciones han colaborado en numerosas actividades, incluyendo las Escuelas de Redes Inalámbricas organizadas anualmente por el ICTP y las de Redes de Computadoras organizadas por EsLaRed en diferentes países de Latinoamérica.

En consecuencia, no fue difícil persuadir al Profesor Sandro Radiciella, jefe del *Aeronomy and Radio Propagation Laboratory* del ICTP que facilitara el viaje de Carlo Fonda en Abril a Venezuela para participar en el experimento.

De vuelta a casa, conseguí un reflector parabólico de malla con iluminación central en casa de un vecino. Su dueño, el Señor Ismael Santos, amablemente nos prestó la antena para realizar los experimentos.

La siguiente figura muestra el desarmado del reflector de malla.



Figura EcLD 5: Carlo y Ermanno desmontando la antena satelital del Sr. Ismael Santos

Cambiamos el iluminador por uno para 2.4 GHz y apuntamos la antena al generador de señales colocado a unos 30 m. Con el analizador de espectros buscamos el máximo de la señal para establecer la posición óptima para el iluminador. Asimismo establecimos la referencia de alineación tanto para la antena con iluminador excéntrico como para la de foco central, como se muestra en la Figura EcLD 6:



Figura EcLD 6: Hallando el foco de la antena con el iluminador de 2.4 GHz

También comparamos la potencia de la señal recibida con la de la salida de una antena comercial de 24 dBi apuntada a la misma fuente, mostrando una diferencia de 8 dB, lo que nos permite concluir que la ganancia total de nuestra antena es de unos 32 dBi.
Por supuesto que este valor no es muy preciso, pues recibimos también señales reflejadas, pero el valor se corresponde a los cálculos realizados a partir de las dimensiones de la antena.

Prospección del sitio de El Baúl

Una vez satisfechos con el funcionamiento adecuado y la manera de apuntar ambas antenas, decidimos realizar una visita al otro extremo del enlace previsto.

Carlo Fonda, Gaya Fior y Ermanno Pietrosemoli llegamos al sitio el 8 de abril. Al día siguiente encontramos una colina al sur del poblado de El Baúl con dos torres de telecomunicaciones pertenecientes a dos operadores de telefonía celular y una tercera perteneciente a la Alcaldía.

Esta colina, llamada Morrocoy, está a 125 m sobre el nivel del mar y unos 75 m sobre el terreno circundante, ofreciendo una ruta sin obstrucción hacia el Pico del Águila.

Hay una carretera de tierra, imprescindible para nuestros propósitos, dado el peso de la antena.

Realización del experimento

El 12 de abril Javier Triviño y Ermanno Pietrosemoli nos desplazamos hacia El Baúl con la antena de iluminación excéntrica cargada en el techo de nuestro vehículo.

Temprano en la mañana del 13 instalamos la antena directamente sobre el borde del terreno en la colina de Morrocoy y la apuntamos al rumbo magnético de 276° ya que la declinación magnética es de 8° y por lo tanto el acimut verdadero es de 268°.

Al mismo tiempo, el otro equipo compuesto por Carlo Fonda y Gaya Fior del ICTP, con la ayuda de Franco Bellarosa, Lourdes Pietrosemoli y José Triviño, trasladaron la antena mallada de 2,7 m al sitio del Pico del Águila previamente identificado.



Figura EcLD 7: Vista aérea de la zona del Pico del Águila con foto del vehículo

El mal tiempo es común a 4100 m de altura, el equipo de el Águila pudo instalar y apuntar la antena justo antes que cayera la neblina y el nevisco.

La figura EcLD 8 muestra la antena con el cordel utilizado para apuntar el haz de radio de 3°.

El generador de señales se alimentó desde el vehículo mediante un inversor de 12 V DC a 120 V AC. A las once de la mañana el analizador de espectros en el Baúl detectó un tono de -82 dBm a la frecuencia previamente acordada de 2450 MHz.

Para asegurarnos de que se trataba realmente de la señal generada en el Águila, le pedí a Carlo que apagara el generador, y la traza del analizador de espectro mostró sólo ruido, confirmando que realmente la señal observada previamente se originaba a unos 280 km de distancia.

Luego de volver a encender el generador de señales, realizamos un ajuste fino de elevación y de acimut en ambos extremos.

Cuando nos convencimos de haber obtenido la mejor señal posible, Carlo sustituyó el generador de señales por un Linksys WRT54G configurado como un AP, mientras Javier sustituía el analizador de espectros en nuestro extremo por otro Linksys WRT54G configurado como cliente.



Figura EcLD 8: Apuntando la antena en El Águila

Enseguida empezamos a recibir "*beacons*" pero los paquetes ping no hallaban respuesta. Esto era de esperarse, puesto que el tiempo de propagación de la onda de radio sobre un trayecto de 300 km es de 1 ms, por lo que el reconocimiento (ACK) a la transmisión de un paquete tarda al menos 2 ms para llegar al transmisor. Afortunadamente, el firmware OpenWRT permite que se ajuste el tiempo de espera por los ACK. Luego de que Carlo realizó el ajuste para compensar el aumento en tres órdenes de magnitud en el tiempo de propagación respecto a los valores estándar de una conexión WiFi, empezamos a recibir paquetes con retardos totales de unos 5 ms.



Figura EcLD 9: Instalación de la antena en El Baúl. La antena está apuntando 1° hacia arriba debido a la iluminación desviada en 22,5°

Procedimos entonces a transferir varios archivos .PDF entre las computadoras de Carlo y de Javier. Los resultados se muestran en la Figura EcLD 10.

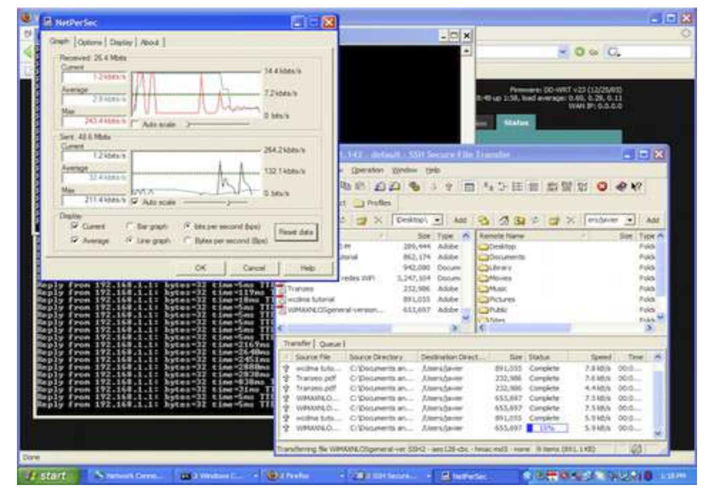


Figura EcLD 10: Pantalla del computador de Javier mostrando detalles de la transferencia de archivos desde el computador de Carlo a 280 km de distancia, usando dos enrutadores inalámbricos WRT54G, sin amplificadores

Note el tiempo de ping de pocos milisegundos.



Figura EcLD 11: Javier Triviño (derecha) y Ermanno Pietrosemoli 'beaming' desde la antena de El Baúl



Figura EcLD 12: Carlo Fonda en el sitio de El Águila

Mérida, Venezuela. 17 de abril de 2006

Un año después de haber realizado el experimento descrito, encontramos el tiempo y los recursos para repetirlo, usando antenas comerciales de 30 dBi y un par de enrutadores inalámbricos modificados por el grupo TIER (*Telecommunication Infrastructure for Emerging Regions*) dirigido por el Dr. Eric Brewer de la universidad de Berkeley. El propósito de la modificación de la capa de acceso al medio estándar de WiFi es hacerla más adecuada para la aplicaciones a grandes distancias reemplazando CSMA (*Carrier Sense Multiple Access*) por TDMA (*Time Division Multiple Access*). Este último es más adecuado para enlaces punto a punto de larga distancia puesto que no requiere el uso de reconocimiento de recepción (ACK). Esto elimina la necesidad de esperar los 2 ms de tiempo de propagación ida y vuelta en un trayecto de 300 km. El 28 de Abril de 2007, un equipo formado por Javier Triviño, José Torres y Francisco Torres instaló una de las antenas en el sitio de El Águila. El otro equipo, compuesto por Leonardo González V., Leonardo González G., Alejandro González y Ermanno Pietrosemoli, instaló la otra antena en El Baúl.Enseguida se logró establecer un enlace mediante los Linksys WRT54G que permitió transmitir video, con un caudal medido de 65 kbps. Cuando reemplazamos los Linksys por los enrutadores inalámbricos que implementan TDMA, el caudal medido subió a 3 Mbps en cada dirección de tráfico, para un total bidireccional de 6 Mbps, concordando con las simulaciones realizadas en Berkeley.

¿Podemos ir más lejos?

Entusiasmados por estos resultados, que permiten avizorar la factibilidad de enlaces de larga distancia a muy bajo costo, el segundo equipo se desplazó hacia otro sitio previamente identificado a 382 km de El Águila, un lugar llamado Platillón, a 1550 m sobre el nivel del mar, que según la simulación realizada con Radio Mobile, permite despejar la primera zona de Fresnel, tal como se puede apreciar en la Figura EcLD 13:

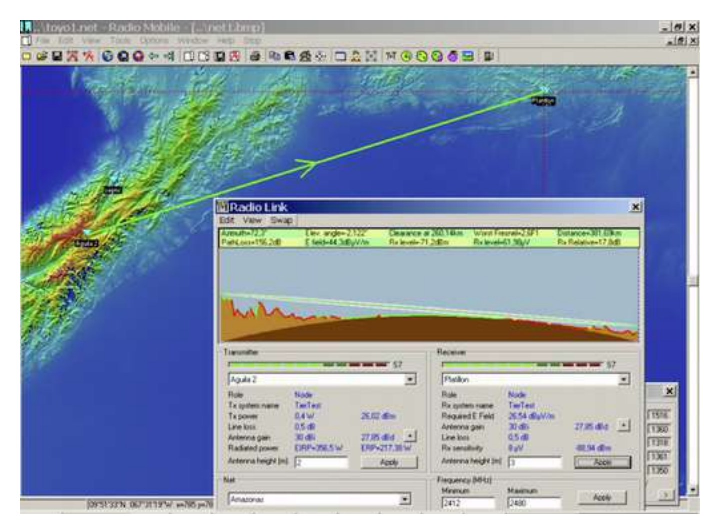


Figura EcLD 13: Mapa y perfil del trayecto de 380 km

De nuevo, se logró rápidamente el enlace tanto con los Linksys como con los enrutadores suministrados por TIER.

Los Linksys arrojaron alrededor de 1% de pérdida de paquetes, con un tiempo de propagación ida y vuelta de aproximadamente 12 ms.

Los enrutadores TIER no registraron pérdidas de paquetes, con tiempos de propagación de 1 ms, lo que permitió transmisión de video, pero el enlace era inestable, notándose significativas variaciones en la intensidad de la señal recibida que a menudo interrumpían la comunicación.

Si embargo, cuando la señal recibida alcanzaba los -78 dBm, el caudal medido fue de 6 Mbps bidireccionales con los enrutadores de TIER que implementan TDMA.



Figura EcLD 14: El equipo de El Águila. De izquierda a derecha: José Torres, Francisco Torres y Javier Triviño

Aunque se requiere realizar otras pruebas para determinar los límites de una tasa de transmisión estable, estamos convencidos de que WiFi tiene un gran potencial para comunicaciones de banda ancha a grandes distancias. Es particularmente adecuado para zonas rurales, donde el espectro no está todavía congestionado y la interferencia no representa un problema, siempre que exista línea de vista despejada.

Agradecimientos

Deseamos expresar nuestra gratitud al Sr. Ismael Santos por prestarnos el reflector mallado utilizado en el Águila y al Ing. Andrés Pietrosemoli por suministrar las uniones para andamios utilizadas para el transporte e instalación de las antenas. También agradecemos al Abdus Salam International Centre of Theoretical Physics por facilitar el viaje de Carlo Fonda de Italia a Venezuela.



Figura EcLD 15: El equipo de Platillón. De izquierda a derecha: Ermanno Pietrosemoli, Alejandro González, Leonardo González V., Leonardo González G.

El experimento de 2006 fue realizado por Ermanno Pietrosemoli y Javier Triviño de EsLaRed, Carlo Fonda y Gaya Fior de ICTP, con la ayuda de Franco Bellarosa, Lourdes Pietrosemoli y José Triviño.

Para el experimento de 2007, el Dr. Eric Brewer de la Universidad de Berkeley suministró los enrutadores inalámbricos con la MAC modificada para largas distancias, así como soporte a través de su colaborador Sonesh Surana.

Se agradece también las colaboraciones de RedULA, CPTM (Corporación Parque Tecnológico de Mérida), la Dirección de Servicios de la ULA (Universidad de los Andes) y Fundacite Mérida.

El segundo experimento fue financiado por el IDCR de Canadá.

Referencias:

Fundación Escuela Latinoamericana de Redes, Latin American Networking School, http://www.eslared.org.ve/
Abdus Salam International Centre for Theoretical Physics,
http://wireless.ictp.it/
OpenWRT Open Source firmware for Linksys,
http://openwrt.org/ www.idrc.ca
Fundacite Mérida,
http://www.fundacite-merida.gob.ve/

--Ermanno Pietrosemoli

Estudio de Casos: Proyecto Pisces

Enlaces Inalámbricos con Energía Solar en Micronesia

Por Bruce Baikie y Laura Hosman, con la asesoría de Marco Zennaro y Ermanno Pietrosemoli del ICTP

Dos enlaces inalámbricos punto a punto, de larga distancia y alimentada con energía solar se instalaron en Micronesia (Pacífico) en agosto de 2012 como parte del proyecto de Conectividad, Educación y Energía Solar de las Islas del Pacífico (PISCES, en inglés).(http://www.piscespacific.org/livesite/), un esfuerzo emprendido por socios múltiples con la finalidad de ofrecer entrenamiento y capacitación local en la región del Pacífico para el uso de las TIC con aprovechamiento de la energía solar.



Figura EcP 1: Formación Práctica

La primera mitad del proyecto PISCES fue un taller de formación práctica sobre la tecnología WiFi de larga distancia usando energía solar en la Universidad de Guam. El taller se concentró en las herramientas de la tecnología WiFi, estándares, energía solar, prospección de sitios, seguridad, y planificación de enlaces. Esta actividad proporcionó muchas oportunidades para la formación práctica, con actividades vespertinas de dos a tres horas de trabajo de laboratorio donde los estudiantes llevaban a la realidad la información teórica impartida en las mañanas. El último día, los estudiantes instalaron un enlace de larga distancia, punto apunto, de energía solar y de banda ancha en el Centro para la Sostenibilidad de la Isla, reemplazando así el viejo y lento enlace a Internet que existía.



Figura EcP 2: Una conexión a Internet más veloz para el Centre for Island Sustainability

Para la segunda mitad del proyecto PISCES, el equipo se trasladó a Chuuk, uno de los Estados Federados de Micronesia (FSM), e instaló una conexión WiFi de larga distancia y energía solar y el Pequeño Laboratorio de Computación Solar, en una escuela primaria de la isla de Udot, Laguna de Chuuc, desconectada hasta ese momento.

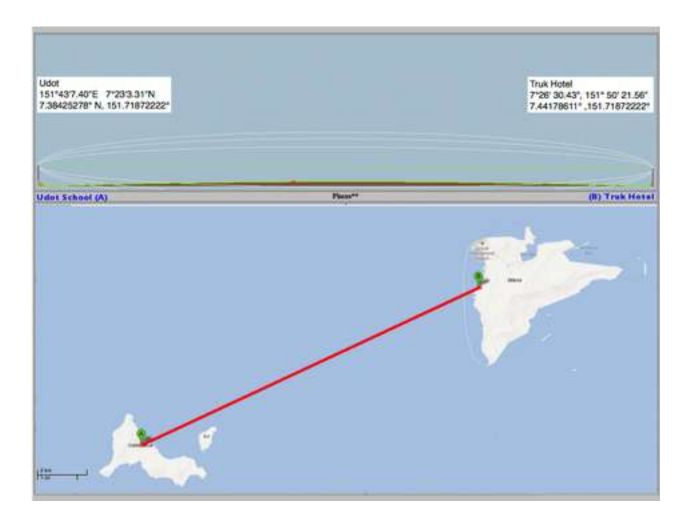


Figura EcP 3: La conexión a Internet para la Escuela Udot se originó en la isla principal de Chuuk, Weno, distante 15 km



Figura EcP 4: Montaje del mástil de la antena en Udot

El equipo Ubiquiti Networks instalado en Weno se montó en el techo del tercer piso del Truk Stop Hotel que tenía la altura necesaria para garantizar la línea visual de la conexión hasta Udot Island sobre la Chuuk Lagoon.
La escuela de un solo piso en Udot, necesitó un mástil de 12 m para montar el otro equipo WiFi Ubiquiti. Los miembros de la comunidad local colaboraron activamente para levantar el mástil, demasiado pesado para ser levantado solamente por el equipo de PISCES. Con miembros del equipo en cada isla, las antenas se alinearon y se conectaron entre sí. La red fue enrutada a través de una conexión local a Internet DSL para dar conectividad a la escuela y a la comunidad local de los alrededores.



Figura EcP 5: Udot

Cada unidad WiFi está alimentada con un sistema fotovoltaico, que consiste en un panel solar de 30 vatios de Solarland EE.UU., un controlador de carga y una batería de 38 amperios hora.

El original “Laboratorio Solar en una Caja” instalado en la escuela de Udot fue desarrollado por estudiantes del Illinois Institute of Technology.
Este laboratorio “llave en mano” fue creado para que fuera de fácil operación en ambientes de energía autónoma.
Incluye seis portátiles “Intel Classmate”, paneles solares y herraje de montaje, controlador de carga, cableado y equipo de seguridad de portátiles; todo esto embalado en una caja de diseño original lista para el transporte y que se transforma en la mesa del laboratorio.



Figura EcP 6: Varias etapas

El proyecto PISCES recibió financiamiento de **Google**, del **Pacific Telecommunications Council**, y la **Internet Society**.

Otros socios de este proyecto son:

- **University of Guam**
- **Illinois Institute of Technology**
- **Green WiFi**, **Inveneo**
- **iSolutions**
- **International Centre for Theoretical Physics (ICTP)**
- **University of California, Berkeley’s TIER research group.**

Estudio de Casos: Red inalámbrica del campus de la University of Ghana

Introducción

La University of Ghana es una de las seis universidades públicas y la universidad más importante de Ghana, con una población de alrededor de 41.000 estudiantes.
Con el creciente número de estudiantes y profesores, era obvio que no podíamos seguir ampliando nuestros laboratorios de informática para facilitar el aprendizaje y la investigación, ya que teníamos poco espacio y limitados fondos para equipar estos laboratorios de computación. La solución consistió en el paso a la tecnología inalámbrica de manera que cualquier estudiante con su computadora portátil pudiera acceder a la red. Sin embargo, esto no se podía lograr inmediatamente por el estado de la red en el momento. Era una gran red plana, sin administración, con un montón de problemas: conflictos de direcciones IP, servidores DHCP independientes (*rogue*), dominios de difusión demasiado grandes, entre otros. Debido a que la unidad de TI no estaba prestando un servicio inalámbrico a la comunidad, los usuarios se impacientaron y comenzaron a conectar sus propios enrutadores inalámbricos a la red. Con esto, la gestión de la red se hacía aún más difícil. Se hizo evidente que si no ofrecíamos un servicio inalámbrico a la comunidad de usuarios, estos iban a encontrar su propia manera de hacerlo. Nuestro primer paso para abordar el problema fue rediseñar nuestra red desde una red plana a una más estructurada, con capas de núcleo, distribución y acceso.

Esto trajo mucha estabilidad a la red. Gracias a los conmutadores (*switches*) administrados, la identificación de problemas llegó a ser mucho más fácil también. La red de cable más estructurada nos dio una buena base para construir una red inalámbrica que la complementara y dar así satisfacción a las crecientes necesidades de nuestros usuarios.

Configuración e instalación de Wifi

Un cierto número de factores se tomaron en cuenta a la hora de escoger el tipo de Punto de Acceso (AP) que se debía utilizar.

Algunos fueron:

- Costo
- Respaldo
- Administración
- Seguridad

Debido al tamaño de nuestra red nos decidimos por una solución empresarial que haría la gestión mucho más fácil. Debido al alto costo de estas soluciones empresariales ($ 600 o más por punto de acceso + costo del controlador) terminamos en un largo debate sobre cuál producto utilizar para la implementación de WiFi. Consultamos entonces el NSRC (*Network Startup Resource Center* de la Universidad de Oregon) que también estaba investigando soluciones inalámbricas asequibles y escalables y nos indicaron los Ubiquiti UniFi, que cuestan alrededor de $ 80 por punto de acceso y tiene un controlador de basado en software gratuito. Junto con el personal de NSRC hicimos un estudio que concluyó con con la instalación piloto con 10 AP. Debido al costo, funcionalidad, facilidad de administración y de despliegue, la Universidad de Ghana decidió incrementar el tamaño del piloto hasta llegar a 90 puntos de acceso UniFi.
Respecto a seguridad, los AP UniFi aceptan tanto WPA Personal como WPA Enterprise, lo que permite a los usuarios autenticarse con un servidor RADIUS. Además de todas las ventajas de implementación de Ubiquiti, encontramos que había una gran comunidad de usuarios UniFi dispuestos a dar ayuda técnica en caso de problemas.

Configuración del AP

La configuración e instalación inicial del AP consistió en conectar el punto de acceso a un puerto del servidor de control perteneciente a la misma VLAN. Para efectos de administración, el AP debe registrarse con el controlador en el proceso denominado adopción. Después de la configuración inicial, el punto de acceso se conecta a la VLAN del switche que da servicio a la red inalámbrica del departamento respectivo.

Direccionamiento IP

Se adoptó el direccionamiento IP privado para la red inalámbrica en el campus. Hay un promedio de 25 subredes inalámbricas en los departamentos, facultades y escuelas.

Ancho de banda

A la red inalámbrica se le asignó el 10% del ancho de banda de la Universidad (STM-1, 155 Mbit/s)

Las nuevas aplicaciones y el uso creciente de la red inalámbrica van a precisar mayor ancho de banda para ofrecer una calidad de servicio adecuada.

Seguridad/Autenticación

Los usuarios y los puntos de acceso se autentican con un servidor RADIUS que usa 802.1x. Tanto los datos de las cuentas estudiantiles como del personal se almacenan en una base de datos MySQL. La red inalámbrica en el campus está en una VLAN separada de la cableada para facilitar la identificación y la gestión.

Conexión a la red inalámbrica del campus de la Universidad de Ghana

La red inalámbrica del Campus de La Universidad de Ghana tiene tres grandes Identificadores (SSID) principales: denominados STAFF, STUDENT, y GUEST.

STAFF

Este SSID es usado por el personal activo de la Universidad.

El personal debe autenticarse usando sus credenciales de identidad personal como nombre de usuario y el PIN como contraseña para ingresar a la red.

STUDENT

Este SSID es usado por los estudiantes de la Universidad que se hayan inscrito en un año académico dado. Los estudiantes se autentican con su identificación de estudiante como nombre de usuario y el PIN como contraseña.

GUEST

La red GUEST está a disposición de los huéspedes que visitan la Universidad por un tiempo determinado.

Los visitantes deben solicitar los detalles de autenticación de su cuenta al departamento de TI.

Fotos de nuestro proyecto e instalación



Figura EcG 1: Nuestro campus



Figura EcG 2: Nuestro campus



Figura EcG 3: Un salón de clase



Figura EcG 4: La biblioteca



Figura EcG 5: Uno de los Puntos de Acceso



Figura EcG 6: Mapa del campus de la Universidad de Ghana con APs



Figura EcG 7: Simulación de la cobertura de las redes inalámbricas con UniFi

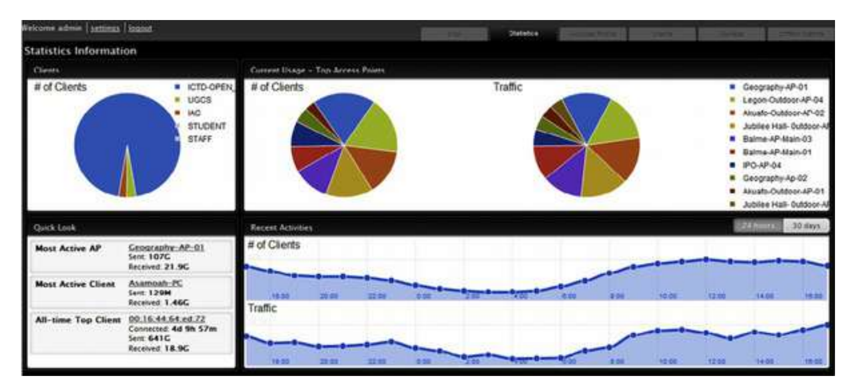


Figura EcG 8: Pantalla del controlador UniFi: estadísticas de uso

Commonwealth-AP-2	10.18.5.5	Connected		0.00	0.00		Restart / Locate
Sabah-Outdoor-AP-02	10.20.3.4	Connected	2	2.85G	1.60G	6 (ng)	Restart / Locate
Akuafo-Outdoor-AP-01	10.21.123.3	Connected	1	27.4G	6.16G	10 (ng)	Restart / Locate
Legon-Outdoor-Ap-01	10.18.3.15	Connected	1	31.0M	12.7M	11 (ng)	Restart / Locate
Legon- Outdoor-AP-02	10.18.3.17	Connected	6	8.71G	1.02G	1 (ng)	Restart / Locate
Commonwealth-AP-3	10.18.5.2	Connected	5	410M	83.8M	11 (ng)	Restart / Locate
Legon-Outdoor-Ap-03	10.18.3.16	Connected (wireless)	10	12.1G	1.43G	1 (ng)	Restart / Locate
REG-AP-3	10.15.3.2	Connected	5	3.27G	215M	11 (ng)	Restart / Locate
Legon-Outdoor-AP-04	10.18.3.18	Connected	6	110G	11.8G	6 (ng)	Restart / Locate
Balme-AP-Main-01	10.21.3.2	Connected	5	63.5G	14.6G	11 (ng)	Restart / Locate
Geography-AP-01	10.14.4.3	Connected	7	105G	20.7G	1 (ng)	Restart / Locate
Chemistry-AP-01	192.168.30.6	Connected	0	261M	26.4M	11 (ng)	Restart / Locate
Geography-Ap-02	10.14.4.2	Connected	1	26.4G	3.97G	6 (ng)	Restart / Locate
IPO-AP-02	10.12.25.80	Connected	5	2.31G	1.63G	1 (ng)	Restart / Locate
ICDE-AP-02	10.12.31.56	Connected	3	5.42G	602M	1 (ng)	Restart / Locate
Sabah-Outdoor-AP-03	10.20.3.3	Connected	4	3.13G	350M	1 (ng)	Restart / Locate
Social_Work-LIB-AP-1	10.17.3.2	Connected	5	1.61G	784M	11 (ng)	Restart / Locate
SON-AP-2	10.18.7.4	Connected	1	332M	86.1M	1 (ng)	Restart / Locate
LAW-AP-01	197.255.120.120	Connected	2	14.5G	1.31G	1 (ng)	Restart / Locate
Jubilee Hall- Outdoor-AP-03	10.20.4.5	Connected	11	23.5G	9.13G	6 (ng)	Restart / Locate
Commonwealth-AP-1	10.18.5.3	Connected	5	3.92G	620M	1 (ng)	Restart / Locate
Geography-Ap-03	197.255.100.7	Connected		0.00	0.00		Restart / Locate
Home_Science-AP-01	10.14.3.2	Connected	2	219M	23.8M	6 (ng)	Restart / Locate
Chemistry-Lib-AP-03	192.168.30.7	Connected	1	1.05G	46.7M	11 (ng)	Restart / Locate
LAW-AP-03	197.255.120.121	Connected	0	7.18G	522M	11 (ng)	Restart / Locate
Commonwealth-AP-4	10.18.5.13	Connected	1	3.97G	271M	6 (ng)	Restart / Locate
Balme-Korea-AP-3							Restart / Locate

Recent Events | Alerts | Settings | Admin

Figura EcG 9: Estadísticas por Punto de Acceso

Name/MAC Address	Status	IP Address	Access Point	Signal	Down	Up	Activity	Uptime	Actions
android_9774d56d682e549c	Authorized	192.168.30.241	Chemistry-AP-02	25%	130K	52.8K		1h 37s	block / unauthorize
UG-IPO-12	Authorized	10.12.25.64	IPO-AP-02	62%	121M	22.2M		5h 4m 29s	block / unauthorize
UG-IPO-08	Authorized	10.12.25.48	IPO-AP-02	45%	39.6M	5.54M		4h 25m 37s	block / unauthorize
UG-IPO-20	Authorized	10.12.25.35	IPO-AP-04	64%	320K	379K		31m 6s	block / unauthorize
UG-IPO-10	Authorized	10.12.25.36	IPO-AP-02	72%	21.8M	1.92M		1h 9m 28s	block / unauthorize
00:0c:e7:00:00:00	Authorized	10.21.123.24	Staff_Resource-Ap-1	0.0%	336	1.15K		8m 39s	block / unauthorize
OBOSUPC	Authorized	192.168.30.165	Chemistry-AP-02	35%	7.78M	1.37M		43m 31s	block / unauthorize
worlali-PC	Authorized	10.18.94.45	SON-AP-1	64%	2.07M	500K		3h 38m 23s	block / unauthorize
SLY-B-PC	Authorized	10.21.3.49	Balme-AP-Main-01	59%	50.9M	4.53M		1h 13m 55s	block / unauthorize
lespie-PC	Authorized	10.17.3.47	NNB2-AP-1	15%	23.2M	3.88M		11m 52s	block / unauthorize
hp-pc	Authorized	10.18.3.176	Legon-Outdoor-Ap-03	27%	8.54M	1.68M		52m 17s	block / unauthorize
ATARE-PC	Authorized	10.14.4.20	Geography-AP-01	57%	52.5M	15.7M		4h 30m 12s	block / unauthorize
KINT-INC-PC	Authorized	10.15.3.18	REG-AP-3	62%	64.9K	91.9K		8m 36s	block / unauthorize
user-2b8162c654	Authorized	10.12.25.92	IPO-AP-01	99%	23.9M	3.10M		1h 5m 30s	block / unauthorize
ubuntu	Authorized	10.21.3.159	Balme-Korea-AP-1	25%	129K	25.2K		26m 53s	block / unauthorize
kwame-PC	Authorized	192.168.30.211	Chemistry-AP-02	50%	31.8M	18.1M		15m 14s	block / unauthorize
gateway-PC	Authorized	197.255.120.18	LAW-AP-04	2.5%	617K	185K		1h 26m 57s	block / unauthorize
pattie-PC	Authorized	10.17.3.85	Social_Work-LIB-AP-1	99%	79.3M	7.46M		3h 1m 58s	block / unauthorize
kofi-2b8b1f1ef5	Authorized	10.20.4.53	Jubilee Hall- Outdoor-AP-03	12%	203K	201K		3h 37m 16s	block / unauthorize
modern-89654cea	Authorized	10.20.4.24	Jubilee Hall- Outdoor-AP-03	82%	5.14M	496K		57m 11s	block / unauthorize
android_9774d56d682e549c	Authorized	10.18.3.30	Pharmacy-Outdoor-AP-2	22%	580K	175K		2h 30m 38s	block / unauthorize
00:18:41:76:89:3b	Authorized		Jubilee Hall- Outdoor-AP-02	20%	815K	132K		4m 52s	block / unauthorize
user-PC	Authorized	169.254.222.47	Commonwealth-AP-4	5.0%	0.00	46.2K		38m 9s	block / unauthorize
SOTTIE-PC	Authorized	10.14.3.22	LECIA-ORID-AP-1	42%	18.4M	1.41M		23m 39s	block / unauthorize
Drew-PC									block / unauthorize

Recent Events | Alerts | Settings | Admin

Figura EcG 10: El controlador también muestra estadísticas por usuario

Retos que enfrentamos

Uno de nuestros principales retos fue conseguir un buen cable CAT5 para la instalación. Además, fue un poco difícil conseguir instalar el cable en la ubicación correcta ya que los edificios no fueron diseñados con este propósito en mente.
El ancho de banda es también un reto, pero estamos tratando de limitar la actividad *peer-to-peer* en la red mediante Cyberoam.

Próximos pasos

Nosotros, el Departamento de IT de la Universidad de Ghana, operamos la red inalámbrica. Tenemos planes inmediatos para expandirla hasta que tengamos la mayor cobertura posible de los edificios de nuestro campus. Esto reducirá la necesidad de que nuestros estudiantes configuren sus propios AP, !lo que hará nuestro trabajo de gestión de la red mucho más fácil!

Autor: Emmanuel Togo, Jefe de la Unidad de Redes del Sistema de Computación de la University of Ghana (UGCS).

Estudio de Casos: Red Airjaldi de Garhwal India

Introducción

En la segunda edición del libro en inglés hemos incluimos un estudio de caso sobre la Red Inalámbrica en Malla de la Comunidad de Dharamsala.
A raíz de esa instalación inicial, en los años siguientes surgió un nuevo conjunto de redes y un ISP inalámbrico comercial en la misma región dirigido por las mismas personas. A continuación se describe uno de sus principales proyectos.

Red Airjaldi de Garhwal:

Trabajando hacia la Viabilidad Económica, y Tecnológica en la Cordillera del Himalaya

Acerca de Rbb/Airjaldi

La Banda Ancha Rural (RBB en inglés) Pvt. Ltd. es un líder innovador e implementador de soluciones de conectividad técnica y económicamente viables para las zonas rurales. Diseña, construye y opera redes de banda ancha en las zonas rurales de la India. Registrado en la India en 2009, RBB actualmente posee y opera redes en los estados indios de Himachal Pradesh, Uttarakhand, Jharkhand y Karnataka. RBB utiliza AirJaldi como un nombre de marca para su red y otras iniciativas relacionadas con la conectividad.
Las actividades de la empresa se llevan a cabo desde nuestra oficina de gestión en Delhi, con oficinas de operación en Dharamsala, Himachal Pradesh y oficinas en otras localidades.
El equipo humano incluye habitantes locales de la India, refugiados tibetanos, profesionales calificados de las áreas metropolitanas de la India y gente de fuera de la India.
Creemos que las redes rurales deben ser técnicamente viables, que necesitan proporcionar una calidad y consistencia de los servicios que sea al menos similar a la ofrecida en cualquier otro lugar.
También tienen que ser económicamente sostenibles: necesitan ser capaces de valerse por sí mismas en un período relativamente corto (unos 18 meses), y al mismo tiempo ofrecer servicios a los clientes a precios razonables.

Además, somos firmes defensores de un enfoque integral "ecosistema minorista": una vez que llegamos a una zona, tratamos de conectar todos los clientes que están en necesidad de conectividad, sin importar el tamaño de su operación o su necesidad de ancho de banda. Aspiramos a que todos nuestros clientes paguen por su conectividad, aunque ofrecemos subvenciones a los clientes seleccionados, principalmente a los dedicados a causas sociales y de desarrollo, y que muestren necesidad económica.

RBB trabaja estrechamente con AirJaldi, Investigación e Innovación, una organización sin fines de lucro según la sección 25 de la legislación India. Creada en 2007, AirJaldi, Investigación e Innovación identifica soluciones de redes adecuadas y asequibles para las zonas rurales, las ensaya en entornos de la vida real y comparte su aprendizaje con organizaciones afines e individuos. AirJaldi también opera un centro de entrenamiento y creación de capacidad en Dharamsala, donde los operadores de la red y los activistas pueden adquirir las habilidades para construir y gestionar redes inalámbricas rurales.

La mayoría de los miembros de nuestro equipo de despliegue han sido entrenados por AirJaldi Investigación e Innovación.
Los miembros del equipo toman normalmente los cursos básicos de un mes "Wireless 108" y el más avanzado “Wireless 216” ofrecidos en la Academia Red AirJaldi. Después de una práctica adicional de 3 meses trabajando en una de nuestras redes bajo la estrecha supervisión de los miembros más antiguos, pasan a ser miembros permanentes del equipo.

Red Airjaldi de Garhwal. Estadísticas principales

Fecha de inicio / arranque | enero 2010
Tamaño/difusión | unos 100 km^2 , que van desde el valle de Dehradun a las alturas de las montañas Tehri Garwal (altura de unos 2.000 metros).
Clientes primarios | Micro banca empresarial, escuelas, organizaciones comunitarias, empresas y usuarios privados.
Enlace Más Largo | 55 kilómetros.
Densidad de población | 169/km^2 (en comparación: Delhi: 9294 / km^2; India general: 363/km ^{2}; EE.UU.: 33,7/km ^{2})

Realidades, necesidades

Los distritos Tehri y Pauri Garhwal de Uttarakhand, que se extienden desde los picos del Himalaya Thalaiya Sagar, Jonli y el grupo Gangotri hasta el Valle Dheradun y Rishikesh, son una de las zonas más montañosas de la India. Conocida por sus muchos templos religiosos a orillas del río Ganges y en las colinas que conducen a la cordillera del Himalaya, esta región es conocida por su ruda belleza. Este aspecto, sin embargo, también es una causa de la pobreza relativa de la región: los habitantes en su mayoría viven en pequeñas aldeas separadas unas de otras por montañas altas y valles profundos. Las principales fuentes locales de ingresos son la agricultura de subsistencia y las industrias artesanales. Muchos de ellos trabajan fuera de la región, en las grandes ciudades, en las llanuras y en las fuerzas armadas y el gobierno de la India.

En 2009, "KGFS Rural Services[2]", una institución de micro-créditos afiliada a IFMR Trust[3], decidió establecer operaciones en esta zona montañosa. Su objetivo era llegar a los clientes potenciales en los pueblos de Tehri y Pauri que hasta entonces tenían poco o ningún acceso a los servicios bancarios regulares e incluso eran considerados como "apenas bancarizables" por la mayoría de los bancos.
Usando mapas de densidad de población, KGFS buscó ubicaciones para sus sucursales bancarias en el centro de las "zonas de influencia" que alcanzaban alrededor de 10.000 personas. Pronto le quedó claro a KGFS que una vez resueltos los pre-requisitos de densidad y accesibilidad, se enfrentaban a graves limitaciones de conectividad, ya que la mayoría de los lugares propuestos no tenían la infraestructura de Internet. La implementación inicial de VSAT y el uso de ADSL locales resultó costosa, lenta y propensa a las averías. Fue entonces cuando recibimos una llamada del equipo de TI de IFMR, preguntando si estaríamos interesados en proponer una solución de conectividad para sus primeras 15 sucursales.

Desarrollo inicial: enfoque, diseño, implementación

Al responder a la llamada, como lo hacemos con peticiones similares, AirJaldi formula su respuesta con base en la información sobre los siguientes elementos:
¿Cuál es la distancia a la troncal de Internet más cercano?

2 http://ruralchannels.ifmr.co.in/kgfs-model/what-is-a-kgfs/
3 http://www.ifmr.co.in/

Nuestros estudios mostraron que había relativamente pocos troncales disponibles en el área.
La mayoría se encontraban en las ciudades de Dehradun y sus vecindades (vea la Figura EcG: 1). Alcanzar desde allí la zona propuesta resultó problemático. Después de mucho esfuerzo localizamos un punto de troncal en una BTS en la ciudad de Narrandar Nagar (ver Figura EcG: 1). Aunque algunas de las sucursales estaban muy cerca de la troncal no había línea visual hacia ella. Esto nos llevó a una solución algo paradójica: utilizar la ubicación Nagar Narrandar como troncal para conectar un Centro de Operaciones de Red (NOC) situado en el valle abajo, donde se facilita la linea visual a las montañas circundantes, potenciales sitios de repetidoras.



Figura EcA 1: Troncal de la red de Garhwal, Centro de Operaciones de Red y algunas sucursales de IFMR, 2009

¿Podíamos proponer un plan de implementación técnicamente sólido, y a la vez asequible para el "cliente de anclaje”[4]" y los clientes adicionales del futuro?
Nuestro estudio inicial de la zona consistió en recoger los datos de latitud y longitud de los sitios de las sucursales propuestas, la identificación de las

4 Cada una de nuestras redes tiene uno o más clientes que se conocen como "clientes de anclaje". El término se refiere a su papel como los primeros clientes en una red, y los que contribuyen principalmente a su viabilidad económica inicial.

posibles ubicaciones de repetidoras, la evaluación del potencial total de clientes en la zona y la evaluación de la infraestructura pública de la zona.

No nos sorprendió que las sucursales se encontraran principalmente en los valles (acceso más fácil para los clientes, cerca de las carreteras) y separados entre sí por cadenas montañosas que impedían la línea visual directa entre ellos.
La fuente de alimentación para las repetidoras prometía ser todo un desafío: los lugares más factibles estaban o fuera de la red o localizados en puntos débiles donde no había energía eléctrica durante días y las fluctuaciones eléctricas violentas hacía que los enrutadores se "colgaran" o se quemaran con los picos de tensión.
Después de tomar la decisión de implementar la red a pesar de todo, nuestro equipo se decidió por la colocación de repetidoras con energía solar en el menor número de puntos estratégicos posible.
Esto llevó a estudios de campo adicionales, lo que implicó horas de investigación de oficina usando mapas topográficos, Google Earth y otras herramientas, seguidos por días de expediciones a los lugares indicados con el fin de ver si un determinado lugar se podía conseguir a través de un acuerdo de alquiler, y para garantizar la seguridad y la integridad de la repetidora por parte de los propietarios de la tierra.

Otra pregunta importante era: ¿cuál es el potencial total de clientes en la zona y va a ser este suficiente para garantizar mínimamente que la red sea económicamente auto-sostenible en unos 18 meses?
El número potencial de clientes no parecía prometedor tampoco.
Además de las sucursales bancarias propuestas encontramos algunos clientes adicionales; principalmente escuelas y otras organizaciones.
Estábamos seguros de que la base de clientes crecería con el tiempo, pero había que encontrar una manera de asegurar la viabilidad en un plazo relativamente corto. Decidimos extender la red a las áreas más densamente pobladas, en las estribaciones de la cordillera de Garhwal.
El trabajo de implementación real se inició en octubre de 2009.
Después de alrededor de dos meses de trabajo de implementación, la red central estaba lista. Su tamaño era de unos 50 x 70 km.
Se proporcionó conectividad a 15 sucursales bancarias y alrededor de cinco escuelas e instituciones en el valle.
La mayoría de sus repetidoras autónomas eran de energía solar y su enlace más largo de un solo salto fue de 54 km.

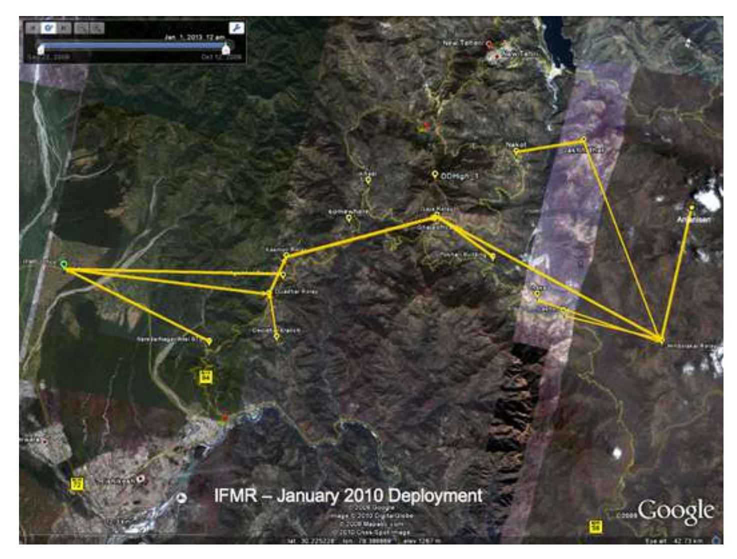


Figura EcA 2: Topología parcial de la Red de Garhwal, 2010



Figura EcA 3: Prospección de campo en la región de Garhwal

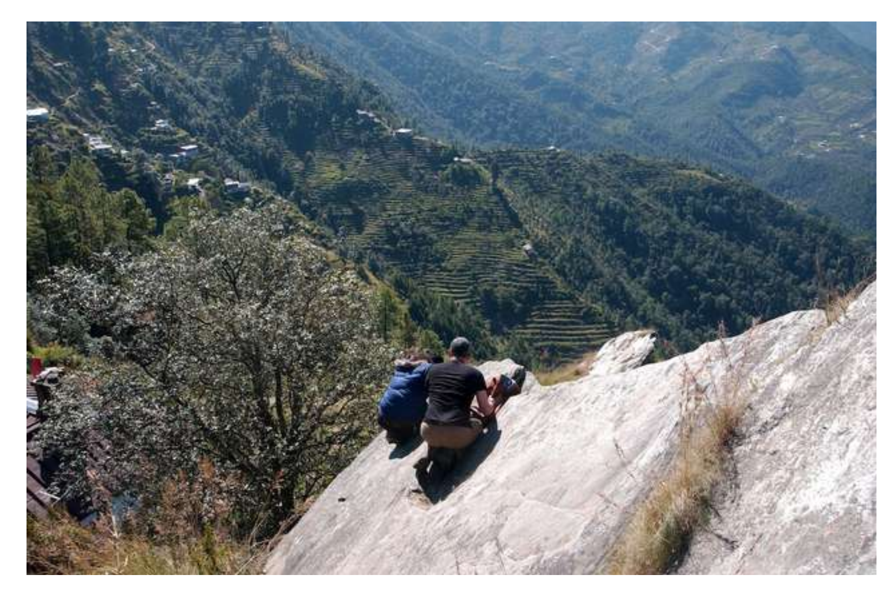


Figura EcA 4: Prospección de campo en Kumaon



Figura EcA 5: Preparativos para instalación de la repetidora. Red de Kumaon



Figura EcA 6: Detección de problemas. Red de Kumaon



Figura EcA 7: Últimos toques a la repetidora solar, Red de Kumaon

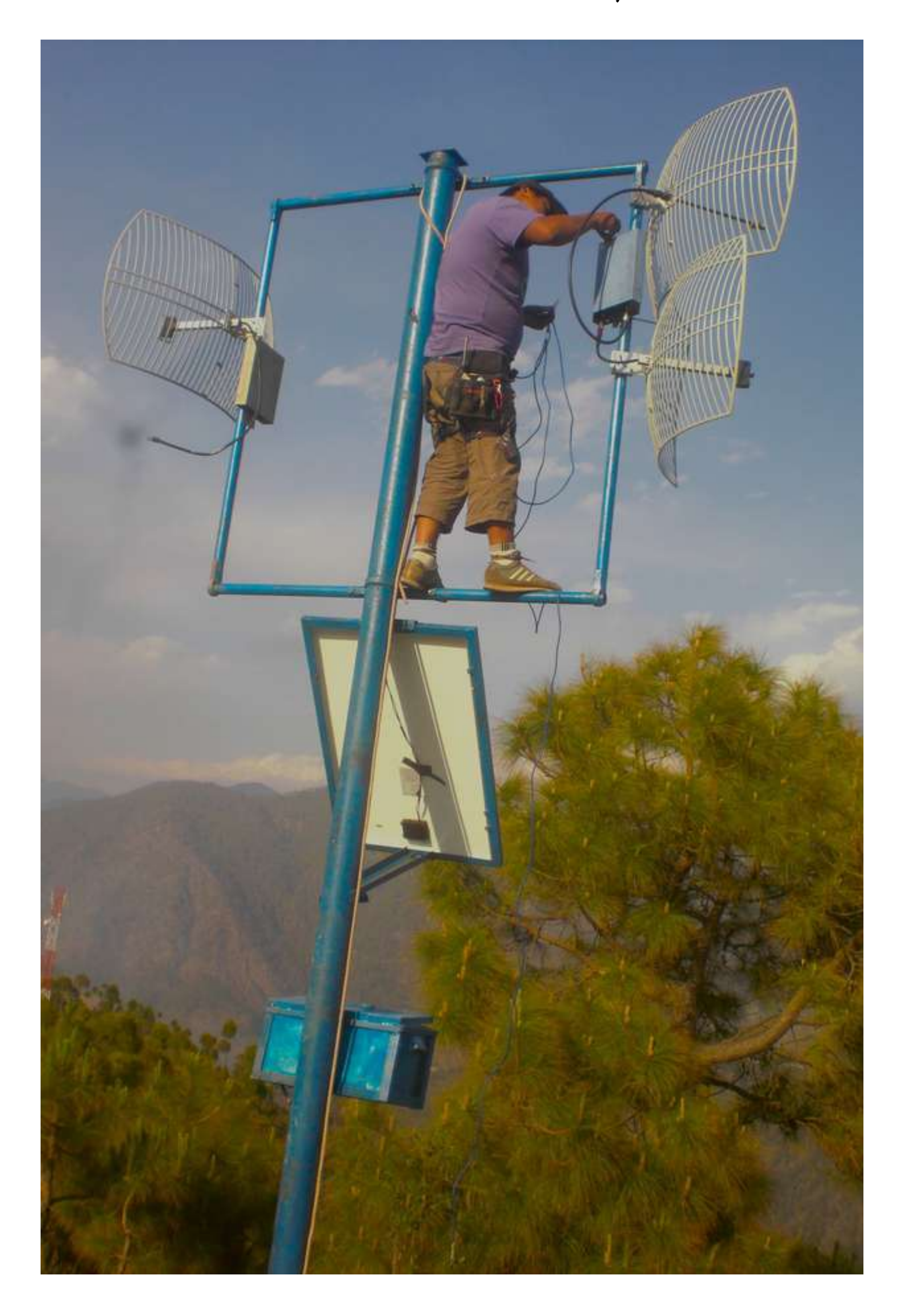


Figura EcA 8: Repetidora Troncal, Red de Garhwal



Figura EcA 9: Repetidora Cliente, red de Kumaon



Figura EcA 10: Repetidora Cliente, Red de Kangra Valley

Tres años después: operación, viabilidad económica retos y respuestas.

Tres años después, la actual red aún abastece a las 15 sucursales iniciales y clientes originales. También ha crecido de manera significativa. Su tamaño actual es de alrededor de 120x100 km. El tiempo de viaje entre nuestra Oficina y Centro de Control de Red y sus confines toma alrededor de !siete horas! Y el número de clientes en las sierras y el valle ha crecido de manera significativa. En sus continuos esfuerzos para mantener esta red tan desafiante, nuestro equipo ha tenido que hacer frente a deslizamientos de tierra, nieve, lluvia, tormentas eléctricas, elefantes salvajes y leopardos (¡sí!). Y, por supuesto, a clientes, para los que gran parte de esto importa poco cuando su línea está caída.

Estamos muy orgullosos del hecho de que nuestro tiempo promedio de red activa en nuestros años de operación en la zona supera el 95% y que la red ha llamado mucho la atención y los elogios de sus usuarios, otros operadores de Internet y los medios de comunicación. Dicho esto, los retos abundan y la lucha por mantener todo en marcha sigue siendo en gran medida un esfuerzo continuo. Los principales retos a los que nos enfrentamos desde el inicio de la red son:

Energía. La energía sigue siendo un gran desafío. El suministro de energía eléctrica es errático y problemático. Aún usando respaldo de baterías, muchos enrutadores se quemaron y se necesitaron muchos viajes para restaurar los enlaces.

La energía solar, por otro lado, aunque casi sin problemas[5] es todavía muy costosa. Asumir nosotros los costos de estas repetidoras es una proposición económica aún más desafiante; pero si los clientes pagan el costo total de una repetidora limitamos el tipo de clientes que pueden aprovechar las conexiones.

Repetidora. Una buena repetidora es una que se coloca en una zona que cubra todo el espacio que sea posible. En el área de Garhwal, esto significa cimas de las montañas. Estos lugares son normal y naturalmente difíciles de encontrar y bastante aislados. La construcción, el mantenimiento y la seguridad de estos sitios es un reto continuo.

---

5 Los meses del monzón con sus lluvias fuertes y sus cielos siempre nublados crean condiciones de carga difíciles y nos han forzado a dotar nuestras repetidoras con capacidad de carga extra, lo que aumenta el costo de las mismas.

En el momento de escribir este artículo estamos ocupados reconstruyendo una repetidora cuyos paneles solares, batería, cargador y otros equipos fueron robados. Algunas de nuestras nuevas conexiones han demostrado ser tan dificultosas como para necesitar una repetidora en cada nueva ubicación con los consiguientes costos.

Tamaño. Aunque estamos orgullosos del tamaño de la red, un recorrido de más de 10 horas entre los dos puntos extremos está agotando al equipo, que se desplaza más que todo en bicicleta, con algunos viajes para solucionar problemas que duran más de dos días.

Viabilidad económica. El modelo dual montaña-valle/baja densidad -alta densidad, ha dado buenos resultados porque en la práctica es un subsidio cruzado, pero no se ha resuelto completamente el problema de la viabilidad económica de las zonas montañosas marginales.
Nuestras respuestas a estos desafíos evolucionan constantemente.

Algunas observaciones actuales y medidas implementadas son:

Energía. Hemos aprendido que las repetidoras de energía solar son la única opción real para la red de Garhwal (como para muchos otros lugares). Al tratar de racionalizar los costos para los clientes hemos limitado nuestra implementación para clientes privados / pequeños negocios a grupos conformados por un mínimo de 10 clientes con una demanda de al menos 1 Mbps por cliente durante un plazo de 5-6 meses. Una densidad más baja, con los consiguientes precios más altos sólo se justifica en el caso de clientes para los que la conectividad es esencial.
También hemos comenzado a implementar los contratos con tiempo mínimo de servicio, es decir, el costo de los equipos de las repetidoras (o su fracción) se amortiza a lo largo de un período de dos años.

Repetidoras. La mejor ubicación no es necesariamente la que tiene la mejor cobertura SOLAMENTE, sino la que presenta una combinación óptima de visibilidad, seguridad, accesibilidad y precio. En ciertos casos, esto significa un mayor número de repetidoras, pero esto es, en general, la opción más barata y racional.

Tamaño. Una solución simple para el problema del tamaño sería fragmentar la red en varias subredes o redes autónomas más pequeñas.

Estamos utilizando este enfoque en otras redes, donde el límite del tamaño va a definirse por un tiempo de viaje máximo de tres horas para visitar cualquier sitio.
Sin embargo, esto no tiene mucho sentido en una red dispersa, como los límites superiores de Garhwal.
La solución de compromiso que encontramos fue la colocación de lugares de almacenamiento en cruces estratégicos de la red. En estos lugares se mantienen los equipos necesarios para atender un área de influencia definida.
Aunque esto no ahorra tiempo de viaje, permite que nuestro personal se mueva rápidamente sin tener que cargar equipamiento pesado y voluminoso.
La transformación de un lugar de almacenamiento en una base de operaciones se producirá cuando mantener un equipo de dos personas en un lugar de ese tipo pueda justificarse por la densidad de clientes y los ingresos.

Viabilidad Económica.

El objetivo primordial de AirJaldi es llegar a las zonas desatendidas y marginadas con conectividad a Internet de alta calidad. Por lo tanto, el modelo de subsidio cruzado se justifica como una solución parcial a los problemas que enfrentan muchos aspirantes a proveedores de Internet rural que carecen de las habilidades o el deseo de construir redes de la escala de la red de Garhwal.

Sin embargo, esto no puede ser la única vía económica para instalaciones en ambientes difíciles. Nuestros intentos de aumentar la viabilidad de la provisión de servicios en zona montañosa incluyen una política agresiva de precios de los paquetes de mayor ancho de banda: el costo marginal por mayor ancho de banda es relativamente bajo, lo que nos permite ingresos marginales más altos, y todavía poder hacer ofertas muy razonables para este tipo de paquetes. Esto contrasta con las soluciones basadas en VSAT y módem inalámbrico que no permiten aumentar el ancho de banda, y constituyen las únicas alternativas a nuestros servicios en estas áreas. En el otro extremo del espectro, hemos comenzado a ofrecer paquetes limitados tiempo / ancho de banda.
Aunque es más caro en costo por unidad, estos paquetes son atractivos para los clientes que desean limitar su consumo a su disposnibilidad económica.

Los planes futuros incluyen la introducción de "4-C": centros locales donde los usuarios pueden utilizar el ancho de banda para aplicaciones de salón de Clase (aprendizaje individual en línea, enseñanza en vivo a un aula, etc.). Cine (ver películas u otros contenidos en línea en un centro local. Café (Café Internet donde la gente puede usar las computadoras individual); y Conectividad (a través de hotspots del área o a través de ofertas de conectividad a casas y oficinas vendidas en el Café).

Resumen

La red Garhwal fue creada en respuesta a una solicitud de un "cliente de anclaje": una empresa de microbanca para la que la conectividad es una condición necesaria para una exitosa implementación de su visión de la banca rural. AirJaldi respondió al desafío con la esperanza de asegurar la alta calidad y la alta disponibilidad de conexión a Internet de banda ancha y la sostenibilidad económica a largo plazo. Estos objetivos se alcanzaron a través de una combinación de planificación detallada, utilización de las ventajas topográficas naturales, expansión de la red desde los terrenos de montaña escasamente poblados hasta el valle de Dheradun con mayor densidad de población, y precios agresivos en los paquetes de mayor ancho de banda. Los planes futuros incluyen la expansión de la red, el "engrosamiento" de la densidad de clientes en las áreas existentes y el enriquecimiento de los paquetes y servicios ofrecidos por AirJaldi.

Estudio de Casos: Open Technology Institute

Red Hook Initiative Wifi y Tidepools

La red inalámbrica *Red Hook Initiative* es una red de malla diseñada en colaboración que ofrece acceso a Internet a la localidad de Red Hook de Brooklyn, NY, y sirve como una plataforma para el desarrollo de aplicaciones y servicios locales. La *Red Hook Initiative* ha construido la red en colaboración con el *Open Technology Institute*, centrando su diseño en el ser humano y haciendo de la participación de la comunidad el núcleo del proyecto. La comunidad expandió la red de manera significativa tras un desastre natural en el otoño de 2012.

Aspectos claves

1. El anclaje principal de la red son las organizaciones comunitarias confiables.
2. Una relación sólida con el proveedor de soporte técnico externo a la comunidad.
3. El proceso de diseño dirigido por la comunidad hace hincapié en las necesidades locales y refuerza el compromiso.
4. El prototipado rápido de aplicaciones diseñadas para la red de área local.

Historia de la red

En el otoño de 2011, la Red Hook Initiative (RHI), una organización de Brooklyn sin fines de lucro enfocada en crear un cambio social a través del compromiso de los jóvenes, se acercó al *Open Technology Institute* (OTI) buscando colaboración para la instalación de una red inalámbrica comunitaria. RHI buscaba una manera de comunicarse con los residentes de inmediato en su centro comunitario. OTI fue inicialmente incapaz de apoyar el esfuerzo de forma directa, pero puso en contacto a Anthony Schloss, Coordinador de Programas de Medios de RHI con Jonathan Baldwin, estudiante graduado de la Escuela de Diseño Parsons quien había estado experimentando con red de malla inalámbrica como plataforma digital local.



Figura EcOTI 1: Viviendas de interés social "Red Hook West"

Red Hook es el ángulo noroeste de Brooklyn que se adentra en la bahía de Hudson. Está separada del resto del barrio por la autopista de Gowanus, que lleva el tráfico de los puntos del sur hacia el bajo Manhattan.

Esta vecindad es el hogar de aproximadamente 5.000 personas provenientes de "Red Hook Houses", conjunto de viviendas de interés social, y de otras zonas de bajos ingresos cerca de una autopista, así como de una sección de nuevas construcciones con muchas empresas pequeñas más cerca del agua.

Muchos sitios industriales, un Ikea y algunos parques públicos completan la zona.



Figura EcOTI 2: Camino desde las oficinas de RHI a la autopista Gowanus



Figura EcOTI 3: La autopista Gowanus que separa la comunidad de Red Hook del resto de Brooklyn

El plan inicial de RHI WiFi era proporcionar acceso inalámbrico a Internet en los alrededores del edificio de RHI, que está cerca de la autopista y el complejo habitacional Red Hook Houses.

Schloss y Baldwin instalaron un Nanostation Ubiquiti en el techo y un enrutador Linksys en el interior del edificio, conectado a través de Ethernet, y conectaron el enrutador Linksys al módem del centro. Esta instalación ofreció una oportunidad para crear prototipos de las primeras versiones de las aplicaciones locales de RHI WiFi. Cuando los residentes o visitantes de RHI se conectaban al punto de acceso inalámbrico llamado "Red Hook Initiative WiFi", eran dirigidos a un sitio web en un servidor local.
En esta página web había una "*Shout Box*", una pizarra digital local de anuncios que permite a la gente dejar un comentario o una nota y participar en el proyecto.

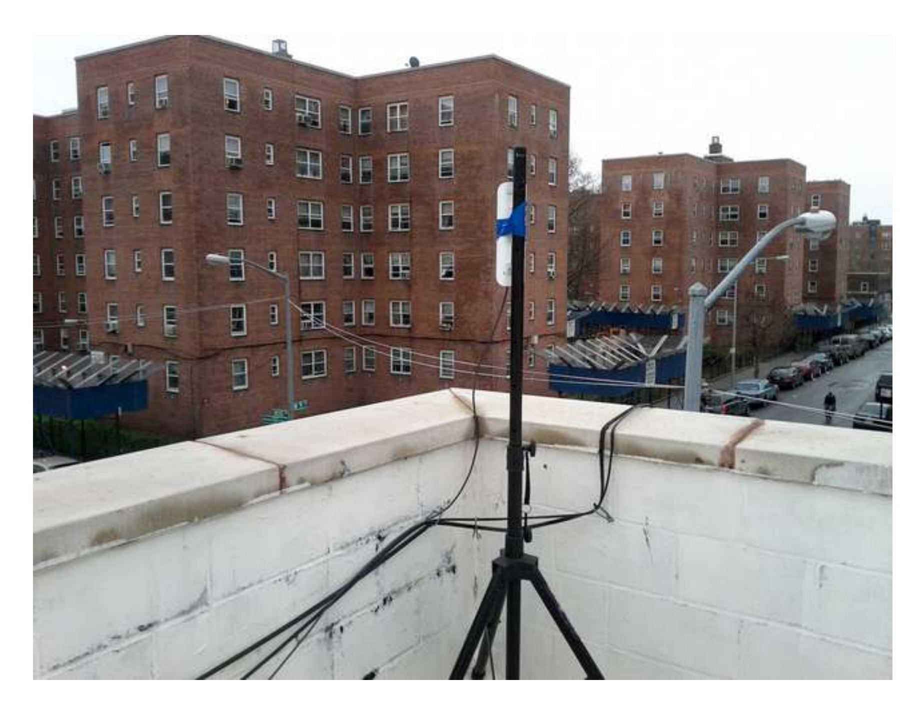


Figura EcOTI 4: Primer nodo WiFi de RHI (Ubiquiti Nanostation) instalado en el techo del edificio de las oficinas de RHI

En marzo de 2012, Baldwin y Schloss instalaron una Nanostation Ubiquiti adicional en el techo de un edificio de apartamentos con vista a Coffey Park y a gran parte del resto del barrio.

Un residente del edificio vinculado socialmente a RHI donó la electricidad y acceso al techo.

Desde este punto panorámico con vista al barrio, la posibilidad de una red inalámbrica para conectar espacios públicos comenzó a tomar forma.

Inicialmente, el punto de acceso inalámbrico de Coffey Park no estaba conectado a Internet, pero se conectó a un servidor GuruPlug.

El servidor básico, de baja potencia alojó una página web local en la red y una "Shout Box" similar a la que funcionaba en RHI.



Figura EcOTI 5: Tendiendo el cable para instalar un nodo en el techo de un edificio al norte de Coffey Park



Figura EcOTI 6: El nodo instalado en el techo del edificio

RHI WiFi utiliza Commotion Wireless un firmware inalámbrico de OTI compatible con los enrutadores Ubiquiti.

Commotion es una herramienta de comunicación libre y de código abierto que utiliza teléfonos móviles, computadores y otros dispositivos inalámbricos para crear redes en malla descentralizadas.
Lo más importante es que Commotion permite que el desarrollo de redes se produzca de forma dinámica y orgánica, de manera que la comunidad puede decidir dónde y cómo debe crecer la red.
Las redes Commotion son sostenibles sin una conexión a Internet, lo que las hace resistentes a los apagones porque pueden distribuir el acceso a las aplicaciones alojadas en servidores locales o en los enrutadores mismos.

El software social y el crecimiento de la red

Basándose en la investigación de redes inalámbricas comunitarias en todo el mundo, Baldwin había identificado la necesidad de un software social que agregara valor y una identidad distinta a la red inalámbrica comunitaria, con los fines concretos de:

- Avivar la participación cívica de la comunidad abordando las necesidades locales, los intereses y la cultura.
- Fomentar la confianza, la interdependencia y la reciprocidad en la comunidad.
- Combinar espacios comunitarios digitales y físicos.
- Asegurar que la gente sepa acerca de las redes en malla y tenga el software instalado antes de que ocurra una interrupción de la comunicación.

Schloss y Baldwin comenzaron a trabajar con los participantes en los programas de los medios de comunicación establecidos de RHI en un proceso de diseño colaborativo, enfocado en las personas y centrado en los conocimientos e intereses de los residentes locales.

A lo largo del primer año, Baldwin y Schloss realizaron talleres con los miembros de la comunidad para determinar las necesidades locales y para reunir ideas de diseño para Tidepools, desarrollado por Baldwin para el ensayo en la red RHI.
Tidepools es una plataforma personalizable de mapeo local y código abierto construido con Javascript, LeafletJS, PHP, MongoDB.

Baldwin lo diseñó para la comunicación local, creación de espacios y organización en torno a los acontecimientos, problemas y recursos de la comunidad.



Figura EcOTI 7: Taller para identificar las necesidades locales para la red RHI WiFi. (Foto de Becky Kazansky)



Figura EcOTI 8: Mapa Tidepools de la red RHI WiFi

Los talleres de la comunidad produjeron ideas para las aplicaciones locales que abordaban las necesidades específicas identificadas por la comunidad. Las necesidades identificadas en los talleres de la comunidad fueron:

- El acceso a Internet (en el hogar, a través de móvil, y en los quioscos del barrio).
- Participación responsable de la comunidad (preguntas frecuentes (FaQ), boletines electrónicos, funcionalidades implementadas mediante SMS).
- El acceso a los recursos (empleo e intercambio de destrezas).
- Sistema de Información Local (archivo histórico, monumentos).
- Multilingüismo (español, árabe y tagalo).
- Interfaz amigable para promover la exploración.

En el verano de 2012, Baldwin se unió al personal de la OTI, y OTI aportó conocimientos adicionales de tecnología a la colaboración, así como su experiencia en el cierre de brechas digitales y en el desarrollo de infraestructuras controladas por la comunidad. La experiencia de la organización en Detroit y Philadelphia proporcionó orientación sobre la manera de colaborar con las comunidades que han sido social, geográfica y tecnológicamente aisladas dentro de las ciudades.

Durante los meses posteriores a las pruebas iniciales de la red local, OTI y RHI se centraron en la realización de tres aplicaciones iniciales que utilizarían la plataforma Tidepools y se ejecutarían en la red inalámbrica local:

- Where's the B61 Bus? : ¿Dónde está el bus B61? Es una aplicación para averiguar los horarios de los buses en tiempo real usando datos de los Horarios de Buses de la API de la Autoridad de Tránsito Metropolitano, (Metropolitan Transit Authority's BusTime API). Fue lanzada el 09 de octubre de 2012.
- Stop & Frisk Survey : La Encuesta Stop & Frisk es una aplicación que los residentes pueden utilizar para documentar las interacciones con la policía en la comunidad de Red Hook y contribuir a mejorar la seguridad pública. Lanzada el 17 de octubre de 2012.
- RHI Radio : Una estación de radio en línea que transmite contenidos producidos por el Grupo de Radio Juventud (Youth Radio Group) de RHI (en desarrollo).



Figura EcOTI 9: Publicidad de "¿Dónde está el Bus B61?". Aplicación de Tidepools



Figura EcOTI 10-11: Interfaz de usuario de móvil para la aplicación "¿Dónde está el bus B61?"

Expansión después del Huracán Sandy

El 29 de octubre de 2012, el Huracán Sandy devastó las zonas bajas de Red Hook, junto con gran parte de la región circundante.
En medio de los apagones e inundaciones, la necesidad de acceso a los

sistemas de comunicación para obtener información sobre lo que estaba pasando y dónde se necesita ayuda fue crucial. El edificio RHI era uno de los pocos lugares que había logrado mantener la energía eléctrica y, en consecuencia, la red WiFi de RHI se había mantenido en pie durante la tormenta. En los días inmediatamente posteriores a la tormenta, hasta 300 personas por día se conectaron a la red para comunicarse con sus seres queridos, saber lo que estaba sucediendo en el resto de la ciudad, y buscar asistencia para la recuperación.

"*Inmediatamente vimos que las comunicaciones son una de las necesidades críticas de la comunidad*", dijo Tony Schloss. "*Queríamos que para la gente fuera lo más fácil posible conectarse a las redes para encontrar vivienda, acceder a la información, o informar sobre su estado de seguridad.*"

La mensajería de texto era el medio -en algunos casos el único- de comunicación mas utilizado por los vecinos del barrio después de la tormenta, por lo que en cuestión de días, OTI desarrolló RHI Status, un plugin SMS a Map para Tidepools usando la API Tropo Application Programming Interface para el manejo de mensajes SMS y la API Google Geocoding para el manejo de direcciones en lenguaje corriente.

RHI Status, les dio a los residentes la posibilidad de enviar un mensaje de texto informando sobre su ubicación y necesidades a un número de contacto, que mapeaba automáticamente la información en Tidepools con las discusiones entrelazadas para que otros usuarios de la comunidad pudieran responder.

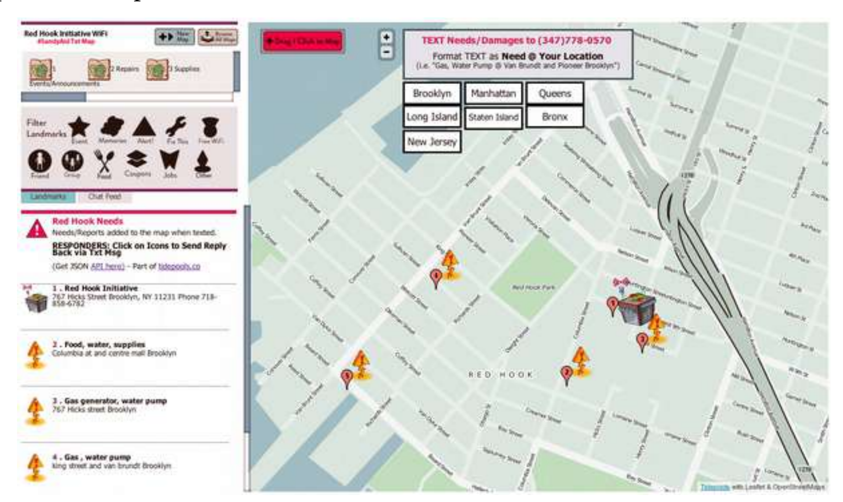


Figura EcOTI 12: Pantallas de la aplicación RHI/Status que traslada mensajes SMS a un mapa Tidepools

A medida que la recuperación progresaba, Frank Sanborn, un Miembro de la *Federal Emergency Management Administration* (FEMA), contactó a RHI para discutir la posibilidad de expansión de la red para los esfuerzos posteriores de recuperación en Red Hook. Sanborn reclutó voluntarios de NYC Mesh y HacDC, un grupo de "hackers" de Washington, en coordinación con el International Technology Disaster Resource Center (ITDRC).
OTI ya tenía una provisión de enrutadores en RHI desde antes de la tormenta.
Con la dirección técnica de la OTI y operando de acuerdo con las metas establecidas por RHI, el equipo instaló un enlace satelital de FEMA en el techo de la RHI, y un enrutador Commotion en el techo de un taller de reparaciones en la manzana de RHI. Anteriormente, el dueño de la tienda se había mostrado reacio a alojar un enrutador ya que no veía un beneficio en ello. Sin embargo, como la comunidad se unió en respuesta a la crisis, el taller de reparaciones se convirtió en un eslabón clave entre la pasarela a Internet de RHI y el enrutador con vista a Coffey Park, que para entonces se había convertido en un importante punto de distribución de ayuda para Red Hook.

Aunque la conexión vía satélite fue puesta por sólo 30 días y proporcionaba un ancho de banda modesto, la red en malla pudo distribuir la conexión a Internet hacia los lugares clave donde los residentes, socorristas y operadores voluntarios más la necesitaban. A medida que la comunidad se unía para responder a la tormenta, se hizo evidente la necesidad de fortalecer una infraestructura las comunicaciones resistente.
Un mes después, con la energía y el agua todavía sin funcionar en gran parte de Red Hook, muchas organizaciones y residentes locales se acercaron a ayudar. "Brooklyn Fiber", un proveedor de servicios de Internet (ISP) local, ofreció una pasarela adicional a RHI WiFi. Para agregar la pasarela a la malla, OTI, RHI y Brooklyn Fiber instalaron un enrutador de 5 GHz Ubiquiti NanoStation Loco que ejecutaba AirOS (conectado a la fibra), y una Nanostation Ubiquiti con Commotion (como un punto de acceso inalámbrico), en el 3er piso del rectorado de la Iglesia de la Visitación en el lado oeste de Coffey Park.
La iglesia también estaba sin energía en ese momento, pero el equipo instaló un uninterruptible power supply (UPS), y que podía hacer funcionar los enrutadores hasta por 12 horas.



Figura EcOTI 13: Nodo del techo. Después de Sandy, otros miembros de la comunidad ofrecieron albergar nodos de la RHI WiFi, y un ISP local donó la conectividad a Internet

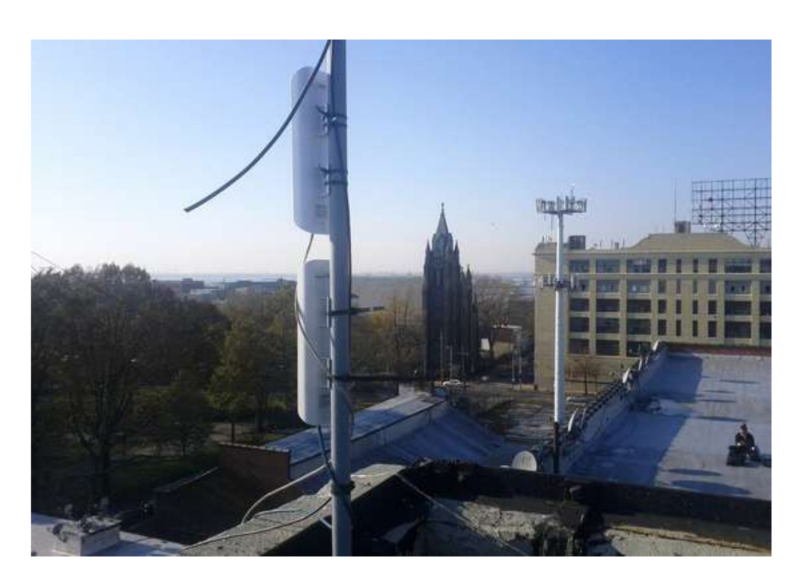


Figura EcOTI 14: Nodo en el techo instalado después de Sandy

Desde la tormenta, RHI WiFi ha apoyado cerca de 100 usuarios por semana, incluso sin la promoción del recurso.
Los datos recogidos por el Commotion sobre las direcciones DHCP asignadas, y los obtenidos de la página de Google Analytics muestran
que los residentes parecen estarse conectando principalmente con dispositivos Android y Apple iPod Touches.
Además, muchos residentes utilizan las estaciones de trabajo en el laboratorio de medios de RHI, así como su conexión inalámbrica. RHI sirve como un anclaje tanto físico como social para la red inalámbrica, impulsando la adopción digital, educando la vecindad y coordinando los esfuerzos de socorro.



Figura EcOTI 15: Mapa de la RHI WiFi. Mapa base (c) Google Maps 2013

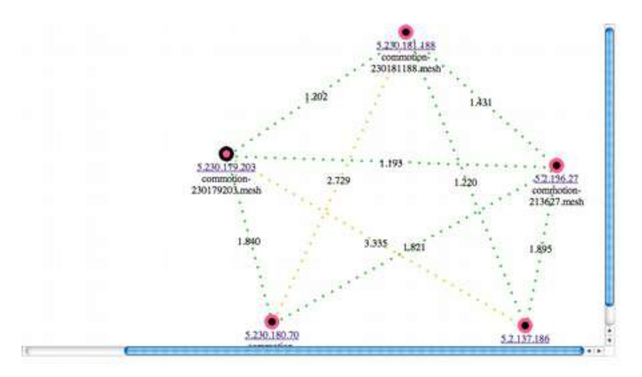


Figura EcOTI 16: Topología de la red en malla vista en OLSRViz

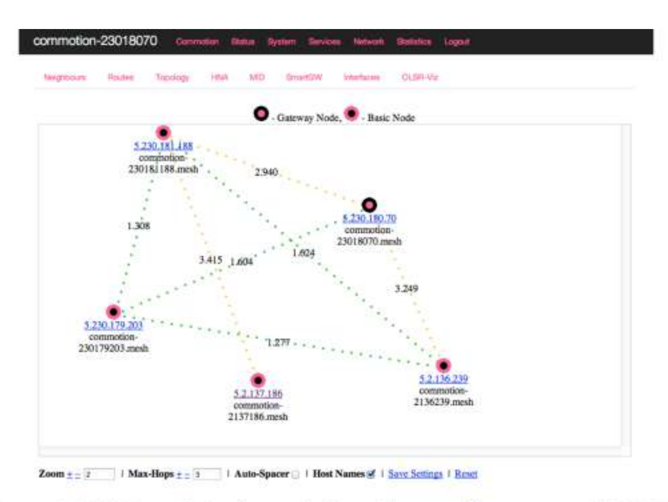


Figura EcOTI 17: Topología de la red en malla vista en OLSRViz

Sostenibilidad y metas futuras

RHI continuará desarrollando el proyecto con el objetivo de apoyar a toda la comunidad en su recuperación del Huracán Sandy.

Con el apoyo de los fondos de Desarrollo Laboral de New York City, RHI y OTI pusieron en marcha un programa de formación en enero de 2013 para involucrar a los residentes locales en el mantenimiento y crecimiento de la red inalámbrica. Siguiendo el modelo del plan de estudios "Digital Steward" elaborado por la OTI y el proyecto Medios Aliados de Detroit, Michigan, el plan de estudios capacitará a los jóvenes para instalar los nuevos enrutadores, mantener los existentes y promover la adopción de la red RHI WiFi en todo Red Hook.

El plan de formación Digital Steward de RHI dará prioridad a los espacios públicos adicionales para la expansión de la red y trabajará con otros residentes en el diseño de nuevas aplicaciones locales. OTI seguirá ayudando en el desarrollo de las aplicaciones y apoyará la construcción de la red en estrecha colaboración con la comunidad.

Costo de la red

Mano de obra donada por los residentes y técnicos locales. El apoyo institucional de RHI y OTI. Hardware (~ $ 50 ~ 85 dólares cada enrutador).

Instalación (3-5 horas de trabajo de dos personas por centro).

Ancho de banda (donado por RHI, Brooklyn Fiber y FEMA). Programa de formación para los residentes locales para mantener y ampliar la red como parte de un programa de empleo municipal.

Lecciones aprendidas

La existencia de los nodos inalámbricos y la red de relaciones humanas antes del desastre facilitó el despliegue rápido de la red a través de:

- Relaciones ya establecidas con los principales interesados de la comunidad.
- Un mayor nivel de alfabetización tecnológica en la comunidad.
- Equipo de red inalámbrica ya existentes en el barrio.

El reto más significativo es la organización inicial y la fase del diseño antes de que se vean los beneficios.
Las aplicaciones diseñadas por la comunidad agregan valor a una red local, incluso en pequeña escala.

Artículos y sitios web relacionados

RELEASE: **New Community-Tech Tool to Help in Sandy's Aftermath**
http://oti.newamerica.net/pressroom/2012/release_new_community_tech_tool_to_help_in_sandys_aftermath

What Sandy Has Taught Us About Technology, Relief and Resilience
http://www.forbes.com/sites/deannazandt/2012/11/10/what-sandy-has-taught-us-about-technology-relief-and-resilience/
A Community Wireless Mesh Prototype in Detroit, MI
http://www.newamerica.net/node/34925

Tidepools
http://tidepools.co
http://www.animalnewyork.com/2012/tidepools-a-social-networktool-in-the-service-of-the-community/
http://wlan-si.net/en/blog/2012/05/26/introducing-tidepools-social-wifi
http://www.core77.com/blog/social_design/a_community-owned_map_accessed_via_mesh_networks_23319.asp
http://www.jrbaldwin.com/tidepoolswifi/

Stop & Frisk App
http://animalnewyork.com/2012/stop-and-frisk-app-launched-by-red-hook-initiative
http://www.dnainfo.com/new-york/20121017/red-hook/stop-and-frisk-app-launched-by-red-hook-initiative

Red Hook
http://www.nycgovparks.org/parks/redhookpark/history